(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 011 222 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.06.2000 Bulletin 2000/25

(51) Int Cl.[7]: **H04L 9/08**

(21) Application number: **99304647.3**

(22) Date of filing: **15.06.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **18.12.1998 JP 36034598**

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

(72) Inventors:
- **Kamada, Jun**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Noda, Bintatsu**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Ono, Etsuo**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Kuroda, Yasutsugu**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Iwase, Shoko**
  Sunnyvale, CA 94086 (US)

(74) Representative: **Fenlon, Christine Lesley et al**
Haseltine Lake & Co.,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

(54) Electronic data storage apparatus with key management function and electronic data storage method

(57) A storage apparatus includes a key management unit (12) for managing an individual key unique to the apparatus and a common key shared with other storage apparatuses, and an encryption unit (13) for performing an encrypting process or verifying data for performing the encrypting process on electronic data stored in the apparatus to which the unit belongs using the individual key, and performing the encrypting process or verifying the data on the electronic data transmitted to or received from another apparatus using the common key. Thus, the apparatus communicates data using an applicable common key in a local environment and a global environment, appropriately manages a key in each environment, and guarantees the security of the electronic data.

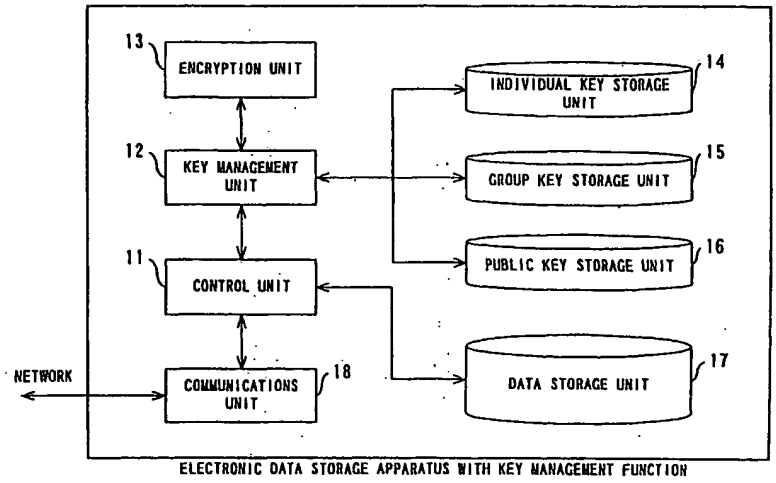

FIG. 2

EP 1 011 222 A2

Description

[0001] The present invention relates to the security of electronic documents, and more specifically to an electronic data storage apparatus with a key management function and an electronic data storage method for guaranteeing the security of electronic data by changing the key used in a process of encrypting electronic data in document form in a local environment and a global environment.

[0002] With an increasing number of electronic transactions and of computers used in official fields, etc., important documents such as contracts, domicile certificates, etc. have come to be processed as electronic data through networks.

[0003] In common contracts and renewal procedures, the originals of documents (contracts, applications, receipts, etc.) and their copies (domicile certificates and their extracts, etc.) are often required. The originals and the copies can be clearly distinguished between them if they are printed on paper because the physical features of paper and ink are different between the originals and the copies. On the similar ground, the originals could not be easily amended.

[0004] However, electronic documents are easily copied to have two same electronic documents, thereby causing the problem that the user cannot tell which is the original document. Therefore, there arises the case where an important document once represented by electronic data is printed onto paper for storage and transfer by mail.

[0005] When an important document is stored or transferred as an electronic document according to a previously-considered method, a common algorithm is used in an electronic data storage apparatus to guarantee the security by performing an encrypting process on the electronic data forming the document. There are two types of keys for use in the algorithm. One is a common encryption using a common key between a transmitter and a receiver of electronic data. The other is a public key encryption using a public key and a private key.

[0006] Thus, in the previously-considered technology, the security of an electronic document is guaranteed by using different keys in an encrypting process between the local environment for electronic data storage devices for storing the same type of electronic data and the global environment for a number of general electronic data storage devices for storing different types of electronic data. However, since a common algorithm is used in the electronic data storage device, the common key is accidentally used in the electronic data storage device in the global environment, and the public key can be used in the local environment.

[0007] As a result, there has been the problem that an authentication station required to manage the public key is operated even on an electronic data storage device to be used only in the local environment, or the reliability on all important documents is lost by the common key disclosed to the electronic data storage devices in the global environment.

[0008] It is desirable to provide an electronic data storage apparatus with a key management function capable of performing a key management process applicable to each environment by transmitting and receiving electronic data after performing an encrypting process on the electronic data using an individual key unique to an electronic data storage device when the device stores the electronic data, and after performing an encrypting process using a common key applicable to either a local environment or a global environment when electronic data is transmitted to or received from another electronic data storage device.

[0009] It is also desirable to provide a method of storing electronic data with the security of the electronic data guaranteed by transmitting to or receiving from another electronic data storage device after re-encrypting using a common key the electronic data already encrypted using an individual key.

[0010] An embodiment of the first aspect of the present invention includes a key management unit for managing an individual key unique to each electronic data storage apparatus, and a common key shared with other electronic data storage apparatuses; and an encryption unit for performing an encrypting process using the individual key on the electronic data stored in each electronic data storage apparatus, and performing an encrypting process using the common key or through data verification on the electronic data transmitted to or received from other electronic data storage apparatuses.

[0011] The key management unit manages a individual key unique to the electronic data storage apparatus to which it belongs, and a common key shared with other electronic data storage apparatuses.

[0012] The encryption unit performs an encrypting process using an individual key on the electronic data stored in the electronic data storage apparatus to which it belongs, and performs an encrypting process or data verification using a common key on the electronic data transmitted to and received from other electronic data storage apparatuses.

[0013] As described above, an encrypting process can be performed using an individual key unique to each electronic data storage apparatus on the electronic data to be stored in it, and an encrypting process and data verification can be performed using a common key shared with other electronic data storage apparatuses on the electronic data transmitted to and received from the apparatuses.

[0014] The common key managed by the key management unit can also be a group key shared in a group of a plurality of electronic data storage apparatuses.

[0015] At this time, a main electronic data storage apparatus may exist in a group, and its own encryption unit may generate an individual key of each of the electronic data storage apparatuses in the group using its own in-

dividual key. The generated individual key can be distributed to each electronic data storage apparatus, or a group key can be generated and distributed. Also, the group key can be generated and distributed by associating a key already assigned to the main electronic data storage apparatus with an externally specified new key.

[0016] Furthermore, there can be an electronic data storage and management apparatus for managing each of the main electronic data storage apparatuses of respective groups. The encryption unit of the apparatus can generate an individual key of each of the main electronic data storage apparatuses using its own individual key, and distribute the generated individual key to the main electronic data storage apparatuses.

[0017] In addition to the group key, the key management unit can also manage a public key as a communications key for use in transmitting data to and receiving data from an electronic data storage apparatus belonging to a group different from the electronic data storage apparatus to which it belongs.

[0018] In addition to the individual key and the common key, the key management unit can also manage a master key common in all electronic data storage apparatuses.

[0019] At this time, using the master key the encryption unit of each electronic data storage apparatus can generate an individual key by encrypting the information identifying the apparatus to which it belongs. When a main electronic data storage apparatus exists in a group, its encryption unit generates a group key by encrypting the information identifying the group using the individual key generated in the apparatus to which the encryption unit belongs, and the generated group key can be distributed to each of the electronic data storage apparatuses in the group.

[0020] Furthermore, a hierarchical structure in which a group of a plurality of electronic data storage apparatuses is defined as one hierarchical level is designed. In this structure, a key management unit can also manage a group key as a common key depending on the hierarchical level of the group of the electronic data storage apparatus to which the key management unit belongs. In a higher order group of electronic data storage apparatuses in the hierarchical structure, there can be an electronic data storage and management apparatus for managing the electronic data storage apparatuses in the group immediately below it. The electronic data storage and management apparatus can generate a group key corresponding to the hierarchical level immediately below it using its own individual key, and distribute the generated group key to the electronic data storage apparatuses in the group immediately below the group of the electronic data storage and management apparatus.

[0021] In an embodiment of a second aspect of the present invention, the electronic data is communicated using a common key shared among electronic data storage apparatuses, and an encrypting process can be performed using the individual key unique to each electronic data storage apparatus on the data to be stored in its own apparatus.

[0022] In a preferred embodiment of the present invention, a group key can be stored as a common key to be shared in a group of a plurality of electronic data storage apparatuses. The electronic data encrypted in the transmitting electronic data storage apparatus using an individual key unique to the apparatus can be re-encrypted using a group key and transmitted to a receiving electronic data storage apparatus. The electronic data received by the receiving electronic data storage apparatus can be verified using the group key. If the electronic data is correct according to the verification, the electronic data can be re-encrypted and stored by the receiving apparatus using the individual key unique to the apparatus.

[0023] Preferably, a public key is stored as a common key to be shared between a electronic data storage apparatus in a group and another electronic data storage apparatus in a different group. Between the above described apparatuses, the transmitting apparatus can re-encrypt and transmit, using a public key, the electronic data encrypted using an individual key and stored in the apparatus, verifies the electronic data received by the receiving apparatus using a private key which is a pair to the public key. If the data is correct according to the verification, then the electronic data can be stored after being re-encrypted using the individual key unique to the receiving electronic data storage apparatus.

[0024] A computer-readable storage medium used in the electronic data storage apparatus embodying a third aspect of the present invention can store a program having the function of verifying the electronic data stored in the electronic data storage apparatus using an individual key unique to the apparatus; and the function of transmitting the electronic data after re-encrypting it using a common key shared with a receiving apparatus if the data is correct according to the verification.

[0025] A computer-readable storage medium used in the electronic data storage apparatus embodying the present invention can store a program having the function of verifying externally received electronic data using a common key shared with a transmitting apparatus; and the function of storing the electronic data after re-encrypting it using the individual key unique to the receiving apparatus if the data is correct according to the verification.

[0026] Reference will now be made, by way of example, to the accompanying drawings, in which:

FIG. 1 is a block diagram illustrating a principle of the present invention;

FIG. 2 is a block diagram of the configuration of an electronic data storage apparatus according to the first embodiment of the present invention;

FIG. 3 is a flowchart of the entire process of an electronic data storage apparatus according to the first

embodiment of the present invention;
FIG. 4 is a flowchart of the process of transmitting and receiving data between electronic data storage apparatuses belonging to the same group;
FIG. 5 is a flowchart of the process of transmitting and receiving data between electronic data storage apparatuses belonging to different groups;
FIG. 6 is a flowchart of the process of storing electronic data when an individual key is preliminarily assigned;
FIG. 7 is a flowchart of the process of managing an individual key of the electronic data storage apparatus by a group master;
FIG. 8 is a flowchart of the process of generating an individual key with two keys associated with each other;
FIG. 9 is a flowchart of managing a group key by a group master;
FIG. 10 is a flowchart of the process of generating a group key with two keys associated with each other;
FIG. 11 is a block diagram of the configuration of an electronic data storage apparatus according to the second embodiment of the present invention;
FIG. 12 is a flowchart of the process of generating an individual key using a master key according to the second embodiment of the present invention;
FIG. 13 is a flowchart of the process of generating a group key according to the second embodiment of the present invention;
FIG. 14 is a flowchart of the process of generating an individual key of a group master by a group management and electronic data storage apparatus;
FIG. 15 shows a hierarchy of groups;
FIG. 16 shows the communications of the electronic data storage apparatuses between a higher order group and a lower order group;
FIG. 17 is a flowchart of the process of transmitting data from a storage apparatus in a higher order group to a storage apparatus in a lower order group;
FIG. 18 is a flowchart of the process of transmitting data from a storage apparatus in a lower order group to a storage apparatus in a higher order group;
FIG. 19 illustrates the storage of an electronic document using an individual key;
FIG. 20 illustrates the process of transmitting and receiving data between two storage apparatuses belonging to the same group;
FIG. 21 shows a method of computing amendment detection information MAC;
FIG. 22 shows a method of generating a key;
FIG. 23 illustrates the generation and the distribution of a group key;
FIG. 24 illustrates a method of managing the entire system through group management SA when there are a plurality of groups each comprising a plurality of SAs; and
FIG. 25 illustrates the loading of a program onto the computer for realizing a electronic data storage apparatus embodying the present invention.

[0027] FIG. 1 is a block diagram illustrating a principle of the present invention. An electronic data storage apparatus 1 shown in FIG. 1 encrypts electronic data using an individual key unique to the apparatus, stores the data, and transmits and receives data using a common key applicable to a local environment or a global environment when an electronic data storage apparatus transmits or receives data between another electronic data storage apparatus.

[0028] In FIG. 1, a key management unit 2 manages an individual key unique to the electronic data storage apparatus to which the unit belongs and a common key shared between the apparatus and another electronic data storage apparatus.

[0029] An encryption unit 3 performs an encrypting process using an individual key on the electronic data stored in the apparatus to which the unit belongs, and performs an encrypting process or data verification using a common key on the electronic data transmitted to and received from another electronic data storage apparatus.

[0030] As described above, according to an embodiment of the present invention, an encrypting process is performed on the electronic data to be stored in each apparatus using an individual key unique to the apparatus, and performs an encrypting process and verification on the electronic data transmitted to or received from another electronic data storage apparatus using a common key shared between the two apparatuses.

[0031] FIG. 2 is a block diagram of the configuration of the electronic data storage apparatus with a key management function according to the first embodiment of the present invention. In the first embodiment of the present invention, an electronic data storage apparatus 10 stores three types of key, that is, an individual key, a group key, and a public key.

[0032] In FIG. 2, a control unit 11 controls the entire operation of the system. A key management unit 12 manages a key stored in the electronic data storage apparatus 10, and an encryption unit 13 generates a key, encrypts electronic data, and verifies the electronic data as necessary.

[0033] An individual key storage unit 14 stores an individual key unique to the electronic data storage apparatus 10 to which the unit belongs. A group key storage unit 15 stores a group key as a common key in a group of a plurality of electronic data storage apparatuses 10. A public key storage unit 16 stores a public key to be used when electronic data is transmitted to or received from an electronic data storage apparatus 10 belonging to another group.

[0034] The electronic data storage apparatus 10 further comprises a data storage unit 17 for storing electronic data, and a communications unit 18 for transmit-

ting and receiving electronic data to and from another electronic data storage apparatus. The communications unit 18 is connected to a network.

[0035] FIG. 3 is a flowchart of the entire process of the electronic data storage apparatus according to the first embodiment of the present invention. In FIG. 3, when electronic data is input or, for example, an instruction to transmit electronic data is input in step S1, it is determined in step S2 whether or not the data is to be stored in the electronic data storage apparatus. The instruction to transmit data input in step S1 is provided from the user of the storage apparatus or an application through, for example, a network.

[0036] When data is to be stored, an individual key stored by the individual key storage unit 14 is selected by the key management unit 12 in step S3, and an encrypting process is performed on the electronic data by the encryption unit 13 using the individual key in step S4. In step S5, the data storage unit 17 stores the data, thereby terminating the process.

[0037] If data is not to be stored in step S2, it is determined in step S6 whether or not the instruction received in step S1 indicates the transmission and reception of data between electronic data storage apparatuses in the same group. If yes, the key management unit 12 selects a group key stored by the group key storage unit 15 in step S7, the encryption unit 13 performs an encrypting process using a group key in step S8, and the communications unit 18 transmits electronic data in step S9, thereby terminating the process.

[0038] If it is determined in step S6 that data is not transmitted or received in the same group, it is further determined in step S11 whether or not data is to be transmitted or received between electronic data storage apparatuses belonging to different groups. If not, the process terminates without proceeding with the process. If yes, the key management unit 12 selects a public key from the public key storage unit 16 in step S12, an encrypting process is performed using a public key in step S8, data is transmitted in step S9, thereby terminating the process.

[0039] FIG. 4 is a flowchart showing the details of the intra-group data transmission and reception process shown in FIG. 3. In FIG. 4, when an intra-group communications instruction is provided for the transmitting electronic data storage apparatus in step S15, data to be transmitted from the data storage unit 17 is selected in step S16, the key management unit 12 selects an individual key stored by the individual key storage unit 14 in step S17, and the encryption unit 13 decrypts the electronic data and verifies the contents of the data using the individual key in step S18. The process performed by the encryption unit 13 is described later in detail.

[0040] If it is determined as a result of the verification of the electronic data that the electronic data has not been amended, then the key management unit 12 selects a group key stored in the group key storage unit 15 in step S19, the encryption unit 13 encrypts the electronic data using the group key in step S20, and the communications unit 18 transmits the data to the receiving electronic data storage apparatus in step S21.

[0041] In the receiving electronic data storage apparatus, the communications unit 18 receives data in step S24, the key management unit 12 selects a group key stored by the group key storage unit 15 in step S25, and the encryption unit 13 decrypts the electronic data and verifies the contents of the data using the group key in step S26.

[0042] If it is determined as a result of the verification that the electronic data has not been amended, then the key management unit 12 selects an individual key stored by the individual key storage unit 14 in step S27, the encryption unit 13 encrypts the electronic data using the individual key in step S28, and the data storage unit 17 stores the data in step S29, thereby terminating the process.

[0043] FIG. 5 is a flowchart of the process of transmitting and receiving data between electronic data storage apparatuses belonging to different groups. Described below are the portions different from those in the flowchart of the process of transmitting and receiving data between electronic data storage apparatuses in the same group as shown in FIG. 4. First, a transmitting electronic data storage apparatus receives an instruction to communicate with an electronic data storage apparatus belonging to a different group in step S31, and a process in steps S16 through S18 is performed similarly as in FIG. 4. Then, the key management unit 12 selects a public key stored by the public key storage unit 16 in step S32, an encrypting process is performed using the public key in step S33, and the result is transmitted to the receiving electronic data storage apparatus in step S21.

[0044] In the receiving electronic data storage apparatus, the key management unit 12 selects a private key which is a pair to a public key stored in the public key storage unit 16 in step S36 after receiving data in step S24, and the encryption unit 13 decrypts the data and verifies the contents of the data using the public key encryption algorithm in step S37.

[0045] If it is verified that no amendments have been made to the electronic data, then the process.in steps S27 through S29 is performed similarly as in FIG. 4, thereby terminating the process. In this case, an electronic document can be processed in a common method such as PEM (privacy enhanced mail) through which an electronic signature is transmitted using a private key from the transmitting apparatus and simultaneously a document encrypted using a public key is transmitted from the receiving apparatus. Otherwise, communications can also be established by temporarily sharing a session key based on the D-H (Diffie-Hellman system) in addition to the public keys of the transmitting apparatus and the receiving apparatus.

[0046] The PEM is an electronic mail system with enhanced security which is proposed as a preferred stand-

ard for the Internet. In the PEM, the DES (data encryption standard) process is used in encrypting a document. The PEM has the feature that a destination can be authenticated.

[0047] The D-H method is a public key distribution method suggested by Diffie and Hellman, and has the feature of secretly sharing a key between two parties.

[0048] As described by referring to FIGs. 4 and 5, when data is transmitted and received between electronic data storage apparatuses in the same or different groups, the data stored after being encrypted using an individual key by the transmitting apparatus is transmitted after being re-encrypted using a group key for the same group, and using a public key for different groups. In the receiving apparatus, data is verified using a group key for the same group, and using a public key for different groups, and is then stored after being re-encrypted using an individual key. As a result, for example, although there is the possibility that a group key is disclosed, the electronic data stored in each electronic data storage apparatus can be secured.

[0049] The flowchart of generating and managing a key stored by each electronic data storage apparatus is described below by referring to FIGs. 6 through 10. FIG. 6 is a flowchart of the data storing process performed when an individual key of each electronic data storage apparatus is preliminarily assigned. A key preliminarily assigned to an electronic data storage apparatus refers to, for example, a key assigned to each apparatus when the electronic data storage apparatus is delivered for sale from a factory. Since the key is managed by its maker, it is called a maker key.

[0050] In FIG. 6, an electronic data storage epparatus having the function of managing a key is generated by its maker in step S40 at the delivery from the factory, and the maker generates a maker key for the electronic data storage apparatus in step S41. In step S42, the electronic data storage apparatus is delivered after the maker key is set in the individual key storage unit 14. The maker key is managed by the maker together with the identification information about the electronic data storage apparatus, for example, its ID.

[0051] When the electronic data storage apparatus is used, electronic data is received in step S44, the key management unit 12 selects the maker key stored by the individual key storage unit 14 in step S45, the encryption unit 13 encrypts electronic data using the maker key in step S46, and the data storage unit 17 stores the data in step S47, thereby terminating the process.

[0052] Thus, by using a maker key managed by the maker as an individual key of an electronic data storage apparatus, it is not necessary for a user to manage a key. In addition, the disclosure of the key can be minimized on the user side. Although the encryption unit 13 of the electronic data storage apparatus on the user side has become out of order, the data in the electronic data storage apparatus can be reconstructed using the maker key managed by the maker.

[0053] FIG. 7 is a flowchart of the process of managing an individual key of an electronic data storage apparatus by a main electronic data storage apparatus in a group, for example, a group master. When the process starts as shown in FIG. 7, a main electronic data storage apparatus, for example, a group master is determined in a group of a plurality of electronic data storage apparatuses in step S50. In step S51, an individual key of each electronic data storage apparatus belonging to the group is generated using the key of the group master. In step S52, the individual key of each electronic data storage apparatus generated by the group master is distributed. In step S53, each electronic data storage apparatus sets the distributed key in its individual key storage unit 14, thereby terminating the process. The method of the group master generating each individual key and distributing the key is described later.

[0054] FIG. 8 is a flowchart of the process of generating an individual key with two keys associated with each other. The two keys refer to, for example, a key preliminarily assigned to an electronic data storage apparatus, and a newly specified key. The preliminarily assigned key is, for example, the above described maker key. The newly specified key is set by a manager who uses the electronic data storage apparatus, and is referred to as a manager key. Unlike a user, a manager can also sets an individual key and a group key. The user can only store, refer to, and transfer electronic data.

[0055] In FIG. 8, when an instruction to generate a new individual key is issued by a manager in step S55, the manager specifies a manager key in step S56, and an individual key is generated with the above described maker key associated with the manager key by the encryption unit 13 in step S57. In step S58, the key management unit 12 sets the generated individual key in the individual key storage unit 14, thereby terminating the process. The process of generating an individual key with a maker key associated with a manager key is described later.

[0056] Thus, by associating a maker key with a manager key when an individual key of an electronic data storage apparatus is generated, a manager can manage electronic data storage apparatuses depending on a change in organization, settings of a group, an environment, and an operation mode. Furthermore, when an encryption unit becomes out of order, the maker can reconstruct and verify data as described above.

[0057] FIG. 9 is a flowchart of managing a group key by a group master. A group key is used in transmitting and receiving electronic data in a group as described above. The flowchart shown in FIG. 9 is the same as the flowchart of the process of managing an individual key by a group master shown in FIG. 7.

[0058] That is, after determining a group master in step S60, a group key is generated by the group master in step S61. In step S62, the group key is distributed to the electronic data storage apparatuses in the group. In step S63, each electronic data storage apparatus sets

the distributed group key in its own group key storage unit 15, thereby terminating the process.

[0059] FIG. 10 is a flowchart of the process of generating a group key with two keys associated with each other as in FIG. 8 in which two keys refer to a maker key and a manager key.

[0060] The first two steps in FIG. 10 are the same as those in FIG. 8. Then, in step S66, the encryption unit 13 generates a group key with a maker key associated with a manager key. In step S67, the key management unit 12 sets a group key in the group key storage unit 15. In step S68, the group key is distributed to the electronic data storage apparatuses belonging to the group, thereby terminating the process. The process according to the flowchart is performed by, for example, the above described group master.

[0061] FIG. 11 is a block diagram of the configuration of the electronic data storage apparatus according to the second embodiment of the present invention. As compared with the configuration according to the first embodiment shown in FIG. 2, an master key storage unit 20 for storing a master key which is a common key shared by all electronic data storage apparatuses is the only difference from the configuration according to the first embodiment.

[0062] FIG. 12 is a flowchart of the process of generating an individual key using a master key according to the second embodiment of the present invention. In FIG. 12, when an instruction to generate an individual key is received in step S70, the identification information about each electronic data storage apparatus, for example, an ID of the electronic data storage apparatus, is obtained by the control unit 11 in step S71, and a master key stored in the master key storage unit 20 is obtained by the key management unit 12 in step S72. In step S73, the encryption unit 13 encrypts the electronic data storage apparatus identification information using the master key, and an individual key is generated. The encrypting process is described later. Then, in step S74, the key management unit 12 sets the generated individual key in the individual key storage unit 14, thereby terminating the process.

[0063] Thus, an individual key can be automatically generated by each electronic data storage apparatus by each apparatus generating each individual key using the master key shared by all electronic data storage apparatuses. In addition, a maker of electronic data storage apparatuses can verify and reconstruct the stored data by referring to the identification information about each electronic data storage apparatus when, for example, its encryption unit becomes out of order.

[0064] FIG. 13 is a flowchart of the process of generating and distributing a group key according to the second embodiment of the present invention. In this process, no master keys are used, and the similar process can be performed according to the first embodiment of the present invention.

[0065] When an instruction to generate a group key is issued to a group master in step S75 shown in FIG. 13, the control unit 11 of the group master obtains group identification information in step S76. The group identification information is an ID for identifying the group managed by the group master. In step S77, the key management unit 12 selects an individual key stored by the individual key storage unit 14, and the encryption unit 13 generates a group key by encrypting the group identification information using the individual key in step S78. In step S79, the generated group key is distributed from the communications unit 18 to the electronic data storage apparatuses in the group.

[0066] In the electronic data storage apparatus which belongs to the group and is managed by the group master, the communications unit 18 receives the group key in step S80a, and the key management unit 12 sets the group key in the group key storage unit 15 in step S80b, thereby terminating the process.

[0067] FIG. 14 is a flowchart of the process of generating an individual key of a group master by a group management and electronic data storage apparatus. A group management and electronic data storage apparatus manages main electronic data storage apparatuses in a plurality of groups, that is; manages a plurality of group masters. The group management and electronic data storage apparatus generates an individual key for each group master, and distributes it to the group master.

[0068] In instruction to generate an individual key of a group master is received in step S82. In step S83, group identification information is specified for each of a plurality of groups. In step S84, the key management unit 12 selects an individual key stored in the individual key storage unit 14. In step S85, the encryption unit 13 encrypts each piece of the group identification information using the individual key, and an individual key for each group master is generated. In step S86, the individual key is distributed to each group master, thereby terminating the process.

[0069] Described below is the hierarchy of groups. For example, in FIG. 3, a plurality of groups of electronic data storage apparatuses are equal to each other according to the first and the second embodiments of the present invention. FIG. 15 shows the case in which a group is designed to form a hierarchy of higher and lower order groups.

[0070] In FIG. 15, a higher order group manages a lower order group to be managed. An electronic data storage apparatus (SA) belonging to the higher order group stores, for example, a higher order group key for the group to which it belongs, and a lower order group key which is a key of the lower order group which it manages. On the other hand, an electronic data storage apparatus belonging to the lower order group stores only the lower group key for the group to which it belongs. Then, for example, in the higher order group, the lower order group master SA for managing the lower order electronic data storage apparatuses generates a lower

order group key and distributes it to the electronic data storage apparatuses SA in the lower order group. The SA is short for a secure archiver, and refers to an electronic data storage apparatus.

[0071] FIG. 16 shows the communicating method between two groups related in a hierarchical structure. The communications between the SAs in a higher order group are established using a higher order group key whereas the communications between the SAs in a lower order group are established using a lower order group key. The communications between an SA of a higher order group, for example, an SA 1, and an SA of a lower order group, for example, an SA 2, are established through a lower order group master SA which is one the SAs of the higher order group and manages the SAs of the lower order group. The communications between the lower order group master SA and an SA belonging to the lower order group, for example, the SA 2 are established using a lower order group key.

[0072] If the lower order group master SA belongs to a management unit of an organization, then a hierarchical group can be realized by the SA of the management unit generating, distributing, and managing an individual key of an SA or a group key of each department, etc. The data stored in each SA can be verified by the management unit.

[0073] FIG. 17 is a flowchart of the process of transmitting data from an SA 1 in a higher order group to an SA 2 in a lower order group. When an instruction to transfer data from the SA 1 of the higher order group to the SA 2 of the lower order group is issued in step S91 shown in FIG. 17, the key management unit 12 shown in FIG. 2 selects an individual key stored in the individual key storage unit 14 in step S92, and the encryption unit 13 decrypts and verifies data using the individual key. Then, the key management unit 12 selects the higher order group key stored in the group key storage unit 15 in step S94. In step S95, the encryption unit 13 encrypts the electronic data using the higher order group key. In step S96, the encrypted electronic data is transferred from the communications unit 18 to the lower order group master SA.

[0074] In the lower group master SA, the communications unit 18 receives the encrypted data in step S97, and the key management unit 12 selects the higher order group key stored in the group key storage unit 15 in step S98. In step S99, the encryption unit 13 decrypts and verifies the electronic data using the higher order group key. In step S100, the key management unit 12 selects the lower order group key stored in the group key storage unit 15. In step S101, the encryption unit 13 encrypts data using the lower order group key. In step S102, the communications unit 18 transfers the encrypted data to a lower order group SA 2.

[0075] In the lower order group SA 2, the communications unit 18 receives the encrypted data in step S103, and the key management unit 12 selects the lower order group key stored in the group key storage unit 15 in step S104. In step S105, the encryption unit 13 decrypts and verifies the electronic data using the lower order group key. In step S106, the key management unit 12 selects the individual key stored in the individual key storage unit 14. In step S107, the encryption unit 13 encrypts data using the individual key. In step S108, the control unit 11 stores data in the data storage unit 17, thereby terminating the process.

[0076] FIG. 18 is a flowchart of the process of transmitting data from a lower order group SA 2 to a higher order group SA 1. The flowchart shows the reverse process of the process shown in FIG. 17. That is, the data transmitting SA 2 performs the process using an individual key and a lower order group key, and the lower order group master SA decrypts and verifies data using a lower order group key, and then encrypts the data using a higher order group key. The receiving SA 1 performs the process using a higher order group key and an individual key.

[0077] In the description of the process shown in FIG. 17, the configuration of the electronic data storage apparatus according to the first embodiment is described. However, the processes shown in FIGs. 17 and 18 are similarly performed in the electronic data storage apparatus according to the second embodiment described by referring to FIG. 2.

[0078] Described below are the methods of storing electronic data (electronic documents) using an individual key, utilizing a group key in a group, generating amendment detection information (message authentication code (MAC)) for the electronic data, generating a key, etc.

[0079] FIG. 19 shows the method of storing an electronic document using an individual key. In FIG. 19, when an instruction to store an electronic document is issued to an electronic data storage apparatus, a MAC is generated using the individual key and the electronic document, and the MAC and the electronic document are stored.

[0080] FIG. 20 shows the process of transmitting and receiving data between two electronic data storage apparatuses belonging to the same group. In FIG. 20, the transmitting electronic data storage apparatus A recomputes the MAC, verifies an electronic document, computes the MAC corresponding to a group key and the electronic document, and transmits the MAC and the electronic document to the electronic data storage apparatus B.

[0081] Then, the electronic data storage apparatus B receives the MAC and the electronic document, verifies the contents of the MAC using the group key, computes the MAC corresponding to the individual key and the electronic document if the verification result is correct, and stores the computed MAC and the electronic document.

[0082] FIG. 21 shows the method of computing amendment detection information MAC for electronic data described by referring to FIGs. 19 and 20. In com-

puting the MAC, the DES (data encryption standard) adopted by the US Standard Institute for use in encrypting electronic data is used. In this encrypting method, the encrypting/decrypting process can be performed by one LSI.

[0083] In FIG. 21, the original data is divided into 64-bit blocks M1, M2, ..., Mn. The DES process is performed on the first 64-bit block M1 using a key, for example, an individual key. An exclusive logical sum of the resultant 64-bit data and the next 64-bit block M2 is obtained.

[0084] Then, the DES process is performed again on the result using, for example, an individual key, and a 64-bit result is obtained. The similar process is continued. Among the resultant 64-bit results, the higher order 32 bits are obtained as the amendment detection information MAC. The computation of the amendment detection information MAC is not limited to the above described method, but can be obtained using other algorithms.

[0085] FIG. 22 shows a common method of generating a key. In FIG. 22, for example, when the above described group master generates and distributes an individual key of an electronic data storage apparatus belonging to its group, the DES process is performed using the information identifying each electronic data storage apparatus, for example, an ID and an individual key of the group master as a seed key. An individual key corresponding to each storage apparatus can be generated and distributed as a new key. As described above, a new key can be similarly generated with two keys, for example, a maker key and a manager key, associated with each other.

[0086] An individual key can be distributed online using a key distributing server or a GKMF (group key management frame work) based on the authentication using a public key. A medium such as a floppy disk, an IC card, etc. can also be used to distribute the key offline.

[0087] The GKMF is performed to set and manage a key by assigning a certificate based on the public key authentication to each group member. The authentication using a public key refers to the system that two parties authenticate each other by obtaining the third party's guarantee (electronic signature) for a public key using an authentication station as the reliable third party.

[0088] FIG. 23 shows the generation and the distribution of a group key. In FIG. 23, for example, there are two groups 1 and 2, and each group has a group master and three subordinate SAs. In FIG. 23, for example, a group master first generates a group master key (Gm key) using its own individual key, an I key, and the ID of the electronic data storage apparatus to which it belongs, then generates a group key and a G key using the Gm key and the ID of the group, and distributes the group key to the subordinate SAs.

[0089] The group key is stored in the group key storage unit in each SA, and managed by a combination of an ID and a key for identifying each group. Normally, plural combinations of a group key and an ID for identifying a group are stored because an SA belongs to a plurality of groups and it is necessary for a lower order group master SA described by referring to FIG. 16 to store a higher order group key and a lower order group key. In addition to a combination of a group key and an ID, an attribute such as the IP address, the name of an electronic data storage apparatus in a group, etc. can be simultaneously managed.

[0090] In FIG. 23, the communications are established between the groups 1 and 2 using a session key (S key). The session key is a private key shared among, for example, group masters based on a public key certificate. A public key is used for communications with a plurality of different groups, managed by a plurality of, for example, group masters as with the case of a group key, and can be stored such that a reliable third party can confirm the authentication based on a public key certificate indicated by the ITU-TX509 of the International Telecommunications Union.

[0091] FIG. 24 shows the method of managing the entire system through group management SA when there are a plurality of groups each comprising a plurality of SAs. In FIG. 24, there are three groups A, B, and C. Each group contains a main electronic data storage apparatus, that is, a group master.

[0092] A group management SA (group management and electronic data storage apparatus) manages group masters SA of respective groups. For example, as shown in FIG. 14, an individual key of a group master SA is generated and distributed to each group master SA. Thus, by providing a group management SA for managing a plurality of groups, communications can be established with any of a number of groups even through a global network such as the Internet, etc.

[0093] Finally described by referring to FIG. 25 is the process of loading a program for realizing the electronic data storage apparatus with a key management function according to the present invention onto a computer. In FIG. 25, a computer 25 stored in a secure case comprises a body 26 and memory 27, and a program can be loaded onto the body 26 from a secure portable storage medium 29. A program can also be loaded from a program provider through a network 28.

[0094] Programs for use in performing various processes in the electronic data storage apparatus within the scope of the claims of the present invention, programs for transmitting and receiving data between electronic data storage apparatuses, and programs shown in each flowchart are stored in, for example, a secure memory 27, and executed by the body 26. The secure memory 27 can be a hard disk, etc.

[0095] Programs for use in transmitting and receiving data between electronic data storage apparatuses are stored in the secure portable storage medium 29, loaded onto the secure computer 25, thereby establishing communications. The secure portable storage medium 29 can be a secure memory card, floppy disk, CD/ROM,

optical disk, magneto-optical disk, etc. Furthermore, programs for establishing data communications can realize the data communications by being loaded after transmitted to the computer 25 in a secure case from a program provider through the network 28.

[0096] The embodiments of the present invention have been described above in detail. However, the present invention is not limited to the above descriptions. It is obvious that the present invention can be represented by various other embodiments.

[0097] As described above in detail, the electronic data storage apparatus has the function of managing a key, thereby storing, transmitting, and receiving electronic data in any applicable environment with the security of important electronic documents guaranteed.

Claims

1. An electronic data storage apparatus (1) for storing electronic data, comprising:

   key management means (2,12) for managing an individual key unique to the electronic data storage apparatus to which said means belongs, and.a common key shared with other electronic data storage apparatuses; and
   encryption means (3,13) for performing an encrypting process on electronic data stored in the electronic data storage apparatus (1) to which said means (3,13) belongs using the individual key, and performing an encrypting process using the common key or with data verification on electronic data transmitted to or received from another electronic data storage apparatus.

2. The apparatus according to claim 1, wherein
   said key management means (2,12) manages a group key as the common key to be shared in a group of a plurality of electronic data storage apparatuses.

3. The apparatus according to claim 1, wherein:

   a main electronic data storage apparatus (group master SA) exists in a group -(group 1) of a plurality of electronic data storage apparatuses;
   said encryption means (3,13) of said main electronic data storage apparatus (group master SA) generates an individual key of each electronic data storage apparatus in the group using an individual key of the apparatus to which said means belongs; and
   said generated individual key is distributed to each electronic data storage apparatus belonging to the group (group 1).

4. The apparatus according to claim 2, wherein:

   a main electronic data storage apparatus (group master SA) exists in the group (group 1);
   said encryption means (3,13) of said main electronic data storage apparatus (group master SA) generates a group key to be shared in the group using an individual key of the apparatus (group master SA) to which said means (3,13) belongs; and
   said generated group key is distributed to each electronic data storage apparatus belonging to the group (group 1).

5. The apparatus according to claim 2, wherein:

   a main electronic data storage apparatus (group master SA) exists in the group (group 1);
   said encryption means (3,13) of said main electronic data storage apparatus (group master SA) generates a group key to be shared in the group with a key preliminarily assigned as the individual key to said main electronic data storage apparatus (group master SA) associated with a new key externally specified; and
   said generated group key is distributed to each electronic data storage apparatus belonging to the group (group 1).

6. The apparatus according to claim 2, wherein:

   a main electronic data storage apparatus (group master SA) exists in the group, and an electronic data storage and management apparatus (group management SA) for managing respective main electronic data storage apparatuses (group master SA) in a plurality of groups (group A, group B, group C) exists;
   said encryption means (3,13) of said electronic data storage and management apparatus (group management SA) generates an individual key of each of said main electronic data storage apparatuses (group master SA) using an individual key of the apparatus (group master SA) to which said means (3,13) belongs; and
   said generated individual key is distributed to each of said main electronic data storage apparatuses (group master SA).

7. The apparatus according to any of claims 2 or 4 to 6, wherein
   said key management means (2,12) manages, in addition to said group key as the common key, a public key for use in transmitting electronic data to and receiving it from an electronic data storage apparatus belonging to a group different from a group of the electronic data storage apparatus to

which said means (2,12) belongs.

8. The apparatus according to any preceding claim, wherein
said individual key is preliminarily assigned to each electronic data storage apparatus (1) before use of the apparatus (1).

9. The apparatus according to any of claims 1 to 7, wherein:
said encryption means (3,13) generates the individual key with a key preliminarily set before use of the apparatus (1) to which said means (3,13) belongs with a new externally specified key; and
said key management means (2,12) manages the generated individual key.

10. The apparatus according to any preceding claim, wherein
said key management means (2,12) manages a master key to be shared by all electronic data storage apparatuses (1).

11. The apparatus according to claim 10, when read as appended to any of claims 1 to 7, wherein: said encryption means (3,13) generates the individual key by encrypting information identifying the apparatus (1) to which said means (3,13) belongs using the master key and
said key management means (2,12) manages the generated individual key.

12. The apparatus according to claim 11, when read as appended to claim 1, wherein: a main electronic data storage apparatus (group master SA) exists in a group (group 1) of a plurality of electronic data storage apparatuses;
said encryption means (3,13) of said main electronic data storage apparatus (group master SA) generates a group key as the common key by encrypting information identifying the group using the generated individual key; and
said generated group key is distributed to each electronic data storage apparatus belonging to the group (group 1).

13. The apparatus according to claim 1, wherein:
a hierarchical structure of electronic data storage apparatuses (1) is designed as having a group of a plurality of electronic data storage apparatuses as one hierarchical level; and
said key management means (2,12) manages a group key as the common key depending on a hierarchical level of a group containing the electronic data storage apparatus (1) to which said means (2,12) belongs.

14. The apparatus according to claim 13, wherein:
in the hierarchical structure of the electronic data storage apparatuses, an electronic data storage and management apparatus for managing electronic data storage apparatuses (lower order group master SA) in a lower order group exists in a group (lower order group) at one level higher than the lower order group;
said encryption means (3,13) of said electronic data storage and management apparatus (lower order group master SA) generates a group key for the lower order group using the individual key of the apparatus (lower order group master SA) to which said means (3,13) belongs; and
said generated group key is distributed to the electronic data storage apparatuses in the group (lower order group) at one level lower.

15. A method of managing electronic data in an electronic data storage apparatus in a hierarchical structure having a group of a plurality of electronic data storage apparatuses as one hierarchical level, comprising the steps of:
a transmitting electronic data storage apparatus (SA1) in one hierarchical level of the hierarchical structure re-encrypting data, encrypted using an individual key which is unique to and stored in the apparatus (SA1), using a higher order group key corresponding to the hierarchical level (S91 to S95), and transmitting the re-encrypted data to an electronic data storage and management apparatus for managing the electronic data storage apparatuses (lower order group master SA) in a group at one hierarchical level lower (S96);
said electronic data storage and management apparatus (lower order group master SA) for managing a lower group of electronic data storage apparatuses (SA2) verifying the received data using the higher order group key (S98 to S99);
re-encrypting the electronic data using the lower order group key corresponding to one hierarchical level lower if the electronic data is correct as a result of the verification (S100 to S101), and transmitting the data to a receiving electronic data storage apparatus (SA2) in the group at one level lower (S102);
said receiving electronic data storage apparatus (SA2) verifying received data using the lower order group key (S103 to S105); and
re-encrypting and storing received data using

an individual key unique to the apparatus (SA2) if the electronic data is correct as a result of the verification (S106 to S108).

16. A method of managing electronic data in an electronic data storage apparatus in a hierarchical structure having a group of a plurality of electronic data storage apparatuses as one hierarchical level, comprising the steps of:

a transmitting electronic data storage apparatus (SA2) in one hierarchical level of the hierarchical structure re-encrypting data, encrypted using an individual key which is unique to and stored in the apparatus (SA2), using a lower order group key corresponding to the hierarchical level (S111 to S115), and transmitting the re-encrypted data to a lower order group electronic data storage and management apparatus (lower order group master SA) for managing the electronic data storage apparatuses (SA2) in the group (S116);
said electronic data storage and management apparatus (lower order group master SA) for managing a lower group of electronic data storage apparatuses (SA2) verifying the received data using the lower order group key (S117 to S119);
re-encrypting the electronic data using the higher order group key corresponding to one hierarchical level higher if the electronic data is correct as a result of the verification (S120 to S121), and transmitting the data to a receiving electronic data storage apparatus (SA1) in the group at one level higher (S122);
said receiving electronic data storage apparatus (SA1) verifying received data using the higher order group key (S123 to S124); and
re-encrypting and storing received data using an individual key unique to the apparatus (SA1) if the electronic data is correct as a result of the verification (S125 to S128).

17. A method of storing electronic data in an electronic data storage apparatus (1) for storing the electronic data, comprising the steps of:

communicating electronic data using a common key shared with other electronic data storage apparatuses (S6 to S12); and
performing an encrypting process using an individual key unique to an electronic data storage apparatus (1) on data to be stored in the electronic data storage apparatus (1)(S2 to S5).

18. The method according to claim 17, wherein

said electronic data storage apparatus (1) stores as the common key a group key shared in one group of a plurality of electronic data storage apparatuses (S15);
a transmitting electronic data storage apparatus transmits electronic data after re-encrypting using the group key the data stored in the apparatus and encrypted using the individual key (S16 to S21);
a receiving electronic data storage apparatus verifies the received electronic data using the group key (S24 to S26); and
when the electronic data is correct according to a result of the verification, said electronic data is re-encrypted using the individual key and stored (S27 to S29).

19. The method according to claim 17, wherein

said electronic data storage apparatus (1) belonging to a group of electronic data storage apparatuses stores as the common key a public key of an electronic data storage apparatus belonging to another group of a plurality of electronic data storage apparatuses (S31);
a transmitting electronic data storage apparatus transmits electronic data after re-encrypting using the public key the data stored in the apparatus and encrypted using the individual key (S16 to S18, S32 to S33, S21);
a receiving electronic data storage apparatus verifies the received electronic data using a private key which is a pair to the public key (S36 to S37); and
when the electronic data is correct according to a result of the verification, said electronic data is re-encrypted using the individual key and stored (S27 to S29).

20. A computer-readable storage medium (27,29) used in an electronic data storage apparatus and storing a program to direct a computer (25) to execute the steps of:

verifying stored electronic data using an individual key unique to the electronic data storage apparatus; and
transmitting the electronic data to a receiving apparatus after re-encrypting the electronic data using a common key shared with the receiving apparatus when a result of the verification is correct.

21. A computer-readable storage medium (27,29) used in an electronic data storage apparatus and storing a program to direct a computer (25) to execute the steps of:

verifying externally received electronic data using a common key shared with a transmitting apparatus of the electronic data; and
re-encrypting the electronic data using an individual key unique to the electronic data storage apparatus and storing the data when a result of the verification is correct.

22. A computer program which, when run on a computer, causes the computer to carry out a method as claimed in any one of claims 15 to 19.

23. A computer program which, when loaded into a computer, causes the computer to become apparatus as claimed in any one of claims 1 to 14.

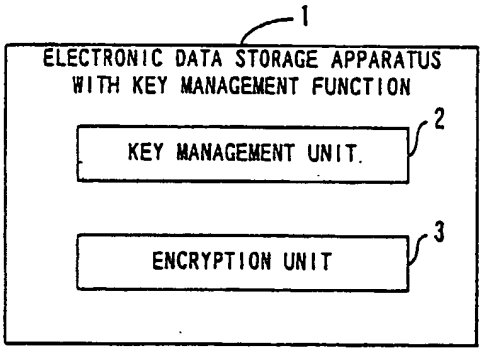
1
ELECTRONIC DATA STORAGE APPARATUS
WITH KEY MANAGEMENT FUNCTION
2
KEY MANAGEMENT UNIT
3
ENCRYPTION UNIT

FIG. 1

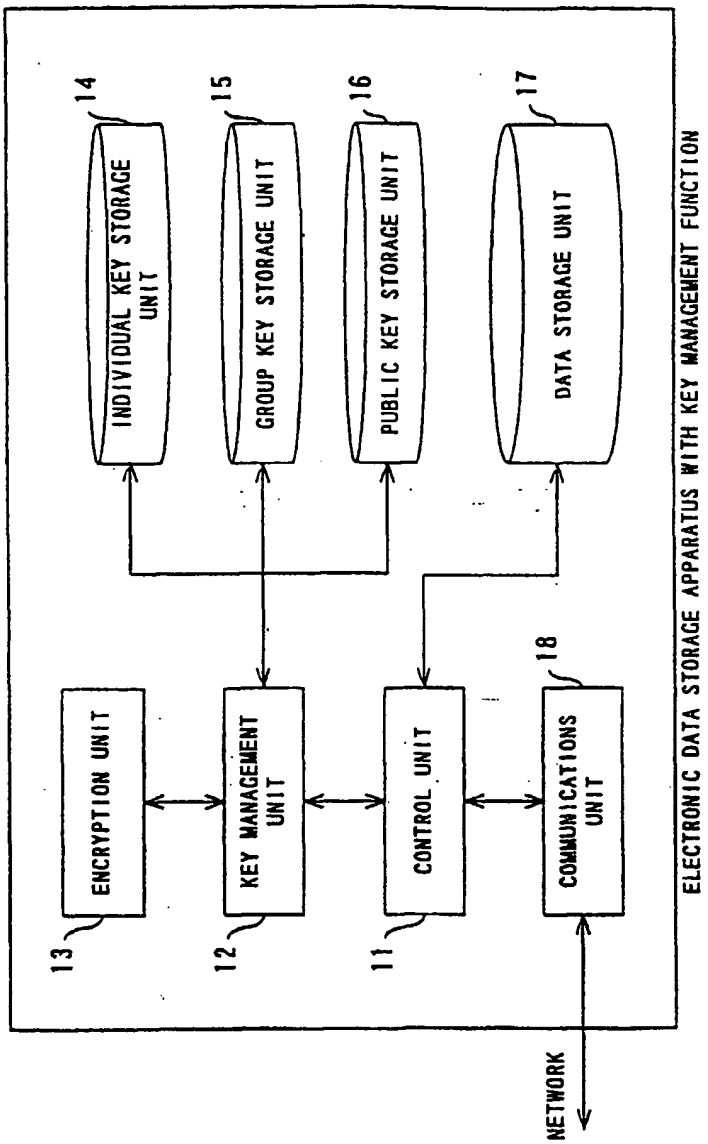
ELECTRONIC DATA STORAGE APPARATUS WITH KEY MANAGEMENT FUNCTION
INDIVIDUAL KEY STORAGE UNIT
GROUP KEY STORAGE UNIT
PUBLIC KEY STORAGE UNIT
DATA STORAGE UNIT
ENCRYPTION UNIT
KEY MANAGEMENT UNIT
CONTROL UNIT
COMMUNICATIONS UNIT
NETWORK
11
12
13
14
15
16
17
18

FIG. 2

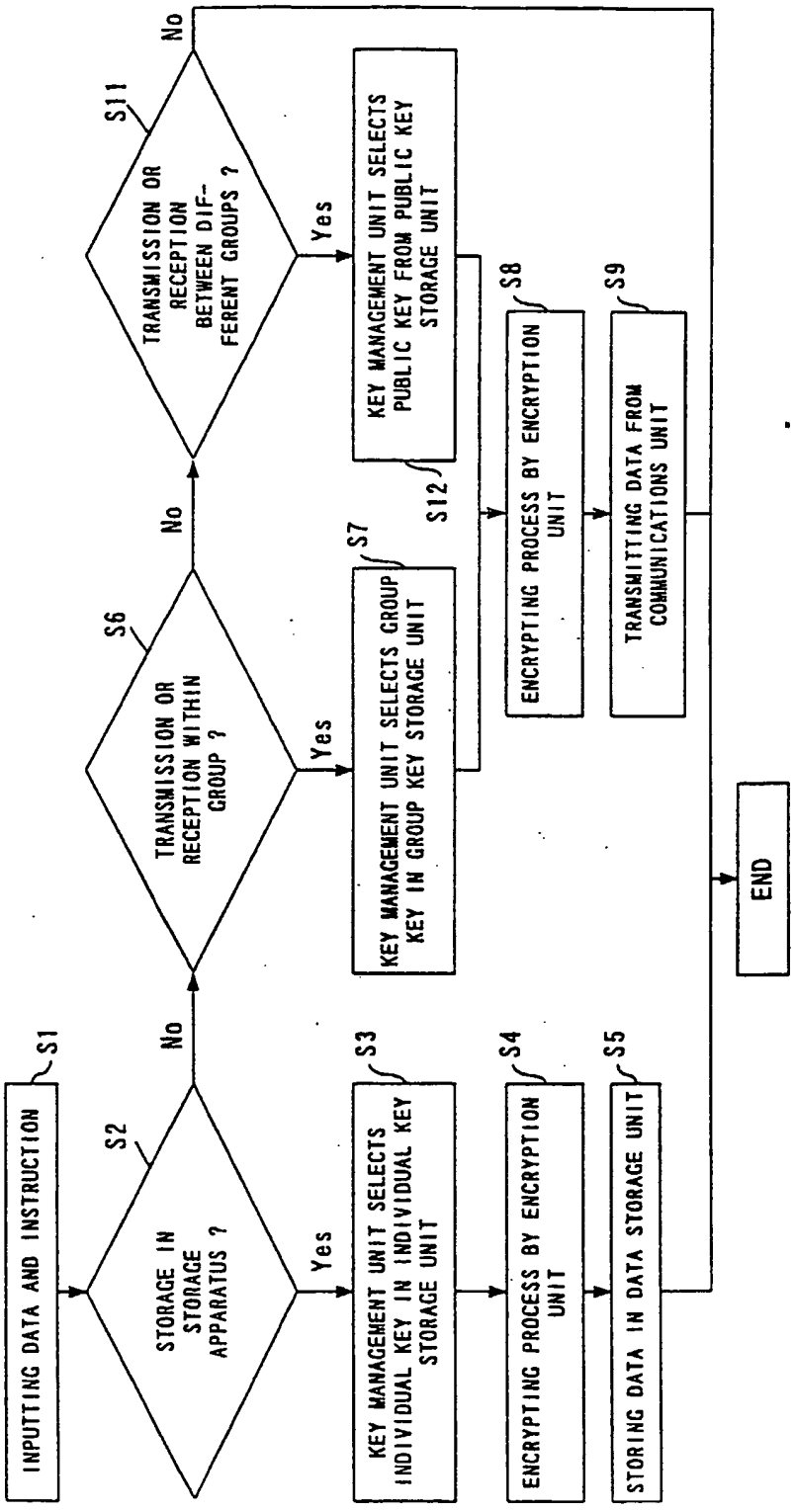
INPUTTING DATA AND INSTRUCTION
S1
STORAGE IN STORAGE APPARATUS ?
S2
Yes
No
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
S3
ENCRYPTING PROCESS BY ENCRYPTION UNIT
S4
STORING DATA IN DATA STORAGE UNIT
S5
TRANSMISSION OR RECEPTION WITHIN GROUP ?
S6
Yes
No
KEY MANAGEMENT UNIT SELECTS GROUP KEY IN GROUP KEY STORAGE UNIT
S7
ENCRYPTING PROCESS BY ENCRYPTION UNIT
S8
TRANSMITTING DATA FROM COMMUNICATIONS UNIT
S9
TRANSMISSION OR RECEPTION BETWEEN DIFFERENT GROUPS ?
S11
Yes
No
KEY MANAGEMENT UNIT SELECTS PUBLIC KEY FROM PUBLIC KEY STORAGE UNIT
S12
END

FIG. 3

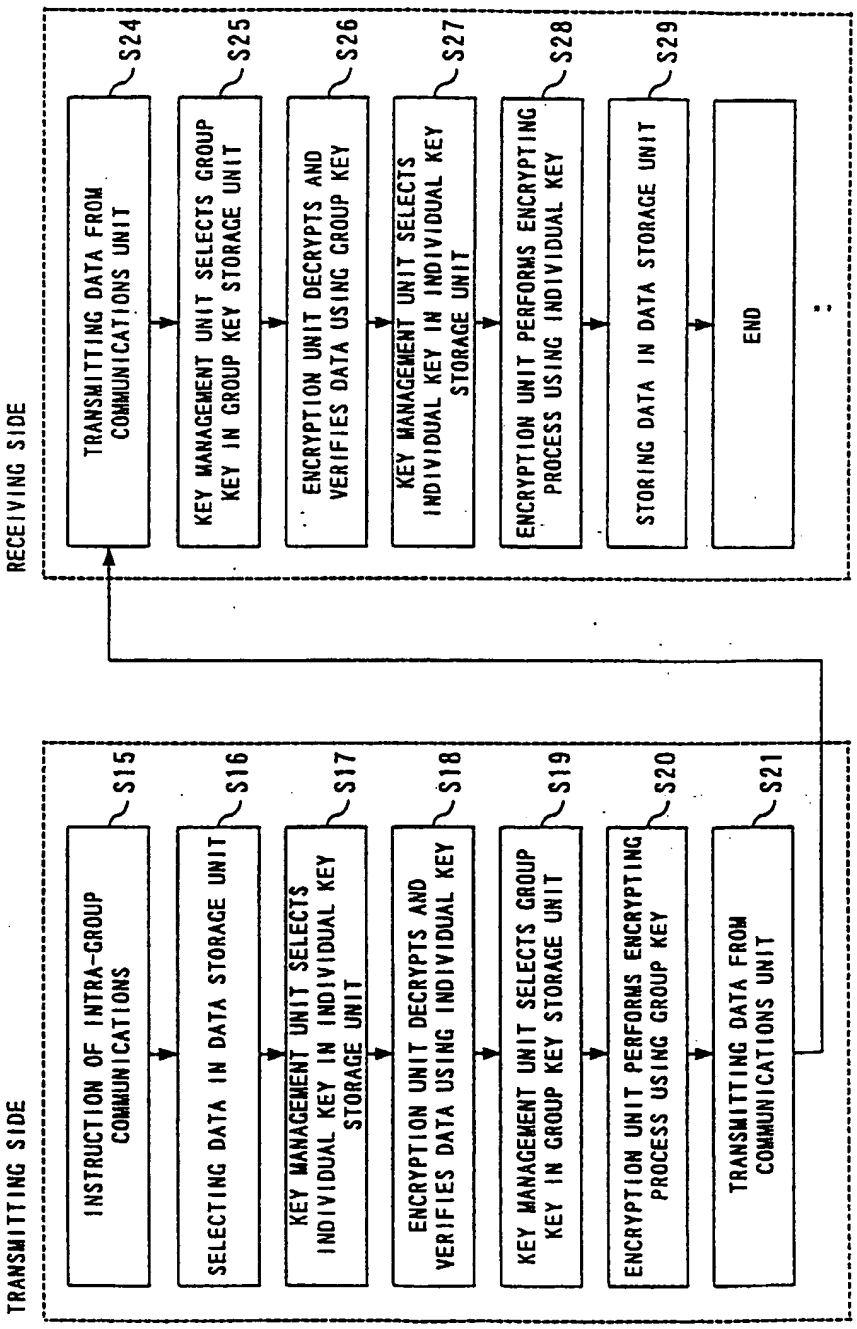
TRANSMITTING SIDE
INSTRUCTION OF INTRA-GROUP COMMUNICATIONS
S15
SELECTING DATA IN DATA STORAGE UNIT
S16
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
S17
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING INDIVIDUAL KEY
S18
KEY MANAGEMENT UNIT SELECTS GROUP KEY IN GROUP KEY STORAGE UNIT
S19
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING GROUP KEY
S20
TRANSMITTING DATA FROM COMMUNICATIONS UNIT
S21
RECEIVING SIDE
TRANSMITTING DATA FROM COMMUNICATIONS UNIT
S24
KEY MANAGEMENT UNIT SELECTS GROUP KEY IN GROUP KEY STORAGE UNIT
S25
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING GROUP KEY
S26
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
S27
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING INDIVIDUAL KEY
S28
STORING DATA IN DATA STORAGE UNIT
S29
END

FIG. 4

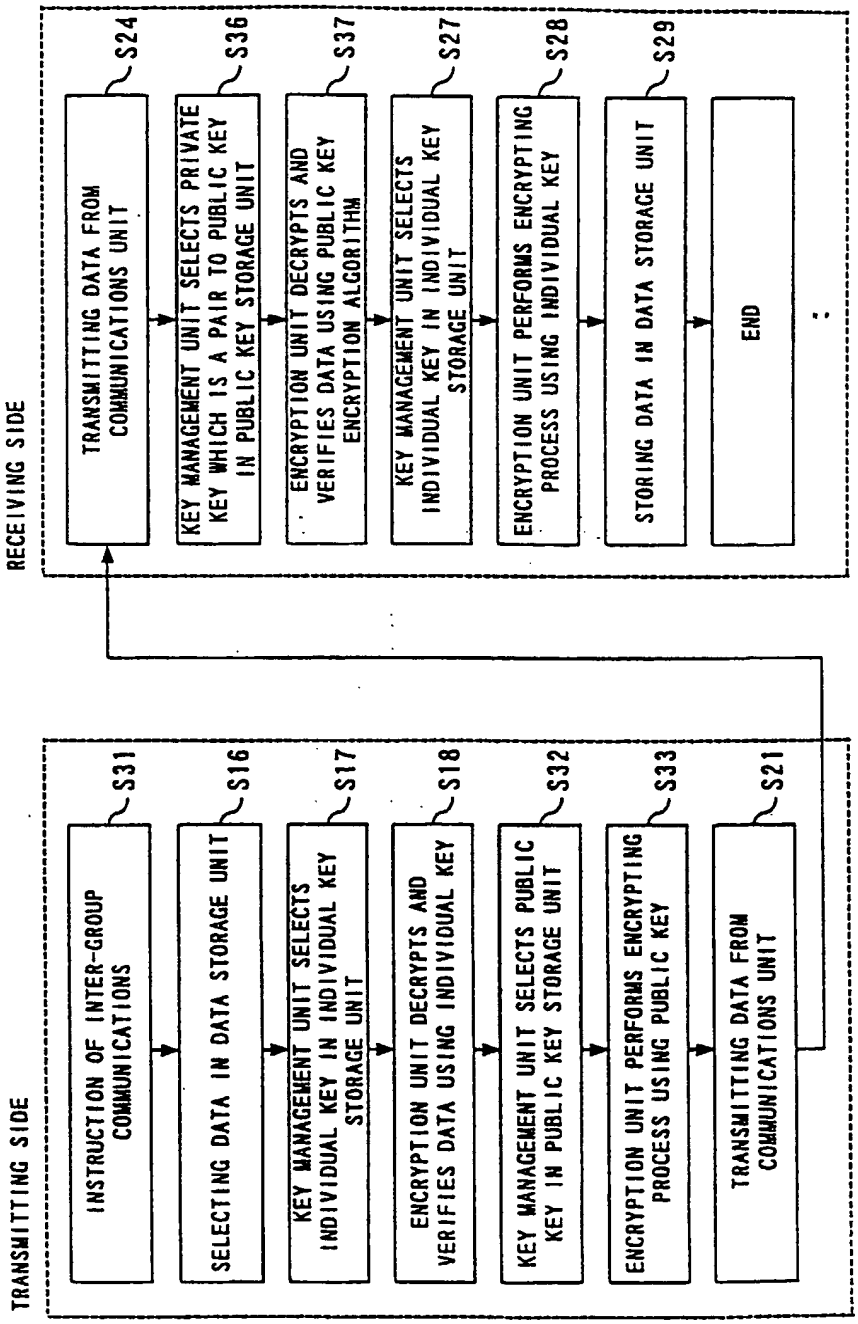
TRANSMITTING SIDE
INSTRUCTION OF INTER-GROUP COMMUNICATIONS
S31
SELECTING DATA IN DATA STORAGE UNIT
S16
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
S17
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING INDIVIDUAL KEY
S18
KEY MANAGEMENT UNIT SELECTS PUBLIC KEY IN PUBLIC KEY STORAGE UNIT
S32
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING PUBLIC KEY
S33
TRANSMITTING DATA FROM COMMUNICATIONS UNIT
S21
RECEIVING SIDE
TRANSMITTING DATA FROM COMMUNICATIONS UNIT
S24
KEY MANAGEMENT UNIT SELECTS PRIVATE KEY WHICH IS A PAIR TO PUBLIC KEY IN PUBLIC KEY STORAGE UNIT
S36
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING PUBLIC KEY ENCRYPTION ALGORITHM
S37
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
S27
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING INDIVIDUAL KEY
S28
STORING DATA IN DATA STORAGE UNIT
S29
END

FIG. 5

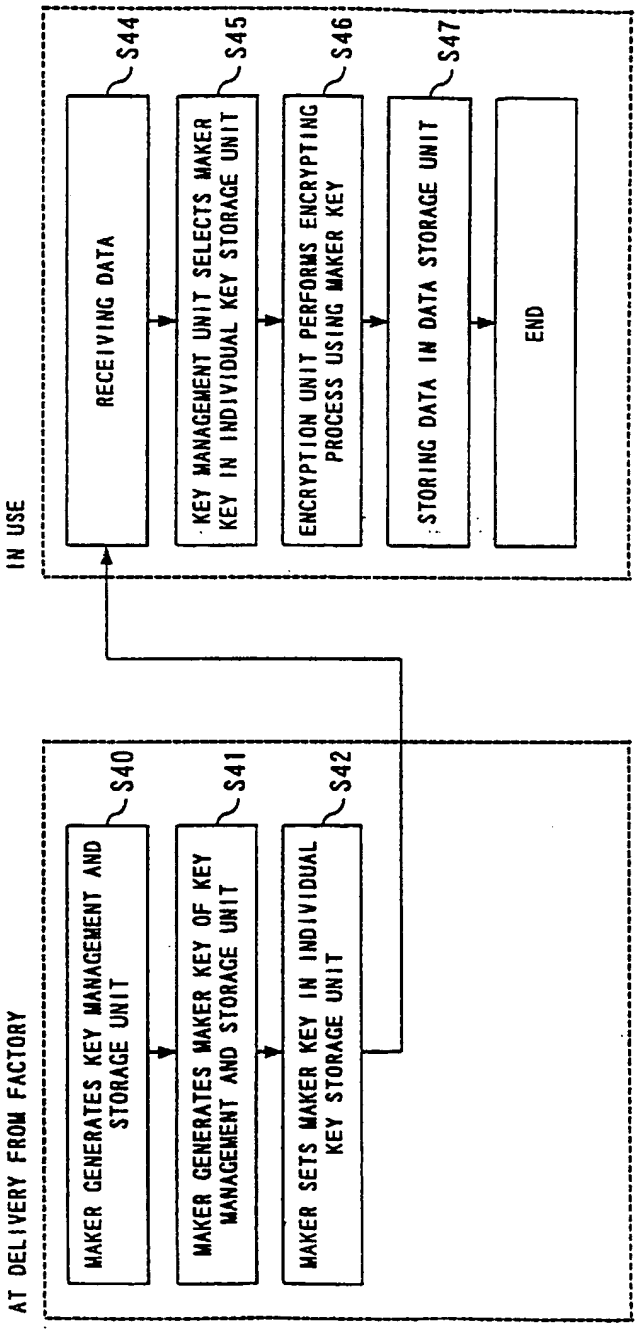
AT DELIVERY FROM FACTORY
MAKER GENERATES KEY MANAGEMENT AND STORAGE UNIT
S40
MAKER GENERATES MAKER KEY OF KEY MANAGEMENT AND STORAGE UNIT
S41
MAKER SETS MAKER KEY IN INDIVIDUAL KEY STORAGE UNIT
S42
IN USE
RECEIVING DATA
S44
KEY MANAGEMENT UNIT SELECTS MAKER KEY IN INDIVIDUAL KEY STORAGE UNIT
S45
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING MAKER KEY
S46
STORING DATA IN DATA STORAGE UNIT
S47
END

FIG. 6

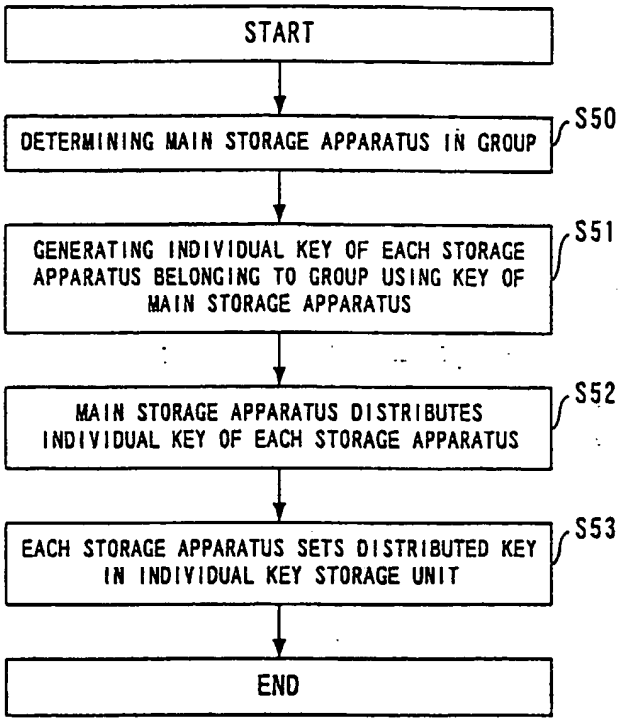
START
DETERMINING MAIN STORAGE APPARATUS IN GROUP
S50
GENERATING INDIVIDUAL KEY OF EACH STORAGE APPARATUS BELONGING TO GROUP USING KEY OF MAIN STORAGE APPARATUS
S51
MAIN STORAGE APPARATUS DISTRIBUTES INDIVIDUAL KEY OF EACH STORAGE APPARATUS
S52
EACH STORAGE APPARATUS SETS DISTRIBUTED KEY IN INDIVIDUAL KEY STORAGE UNIT
S53
END

FIG. 7

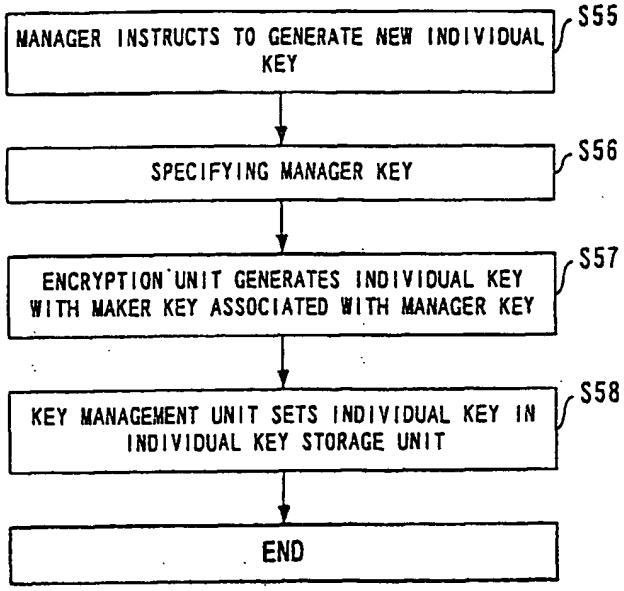
MANAGER INSTRUCTS TO GENERATE NEW INDIVIDUAL KEY
S55
SPECIFYING MANAGER KEY
S56
ENCRYPTION UNIT GENERATES INDIVIDUAL KEY WITH MAKER KEY ASSOCIATED WITH MANAGER KEY
S57
KEY MANAGEMENT UNIT SETS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
S58
END

FIG. 8

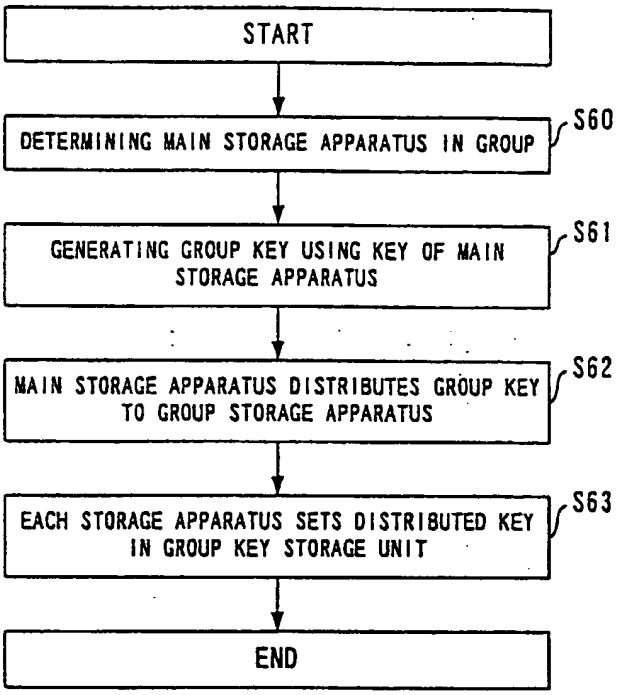
START
DETERMINING MAIN STORAGE APPARATUS IN GROUP
S60
GENERATING GROUP KEY USING KEY OF MAIN STORAGE APPARATUS
S61
MAIN STORAGE APPARATUS DISTRIBUTES GROUP KEY TO GROUP STORAGE APPARATUS
S62
EACH STORAGE APPARATUS SETS DISTRIBUTED KEY IN GROUP KEY STORAGE UNIT
S63
END

FIG. 9

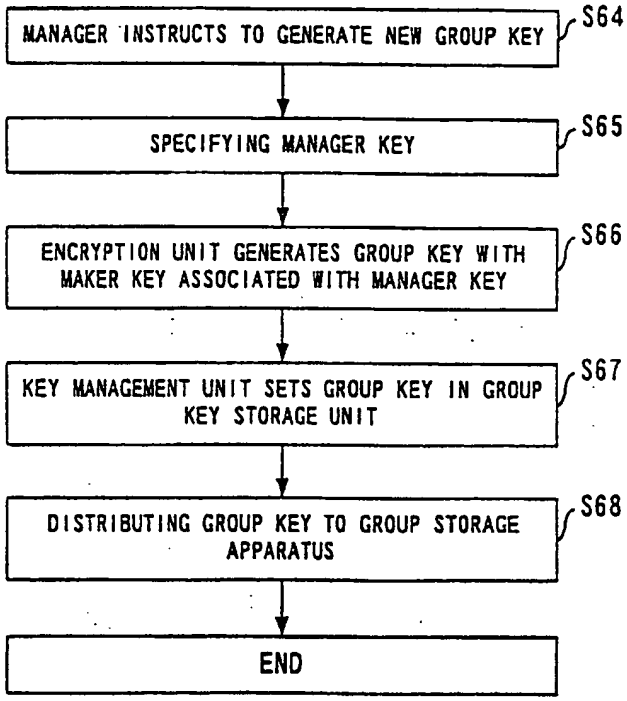
MANAGER INSTRUCTS TO GENERATE NEW GROUP KEY
S64
SPECIFYING MANAGER KEY
S65
ENCRYPTION UNIT GENERATES GROUP KEY WITH MAKER KEY ASSOCIATED WITH MANAGER KEY
S66
KEY MANAGEMENT UNIT SETS GROUP KEY IN GROUP KEY STORAGE UNIT
S67
DISTRIBUTING GROUP KEY TO GROUP STORAGE APPARATUS
S68
END

FIG. 10

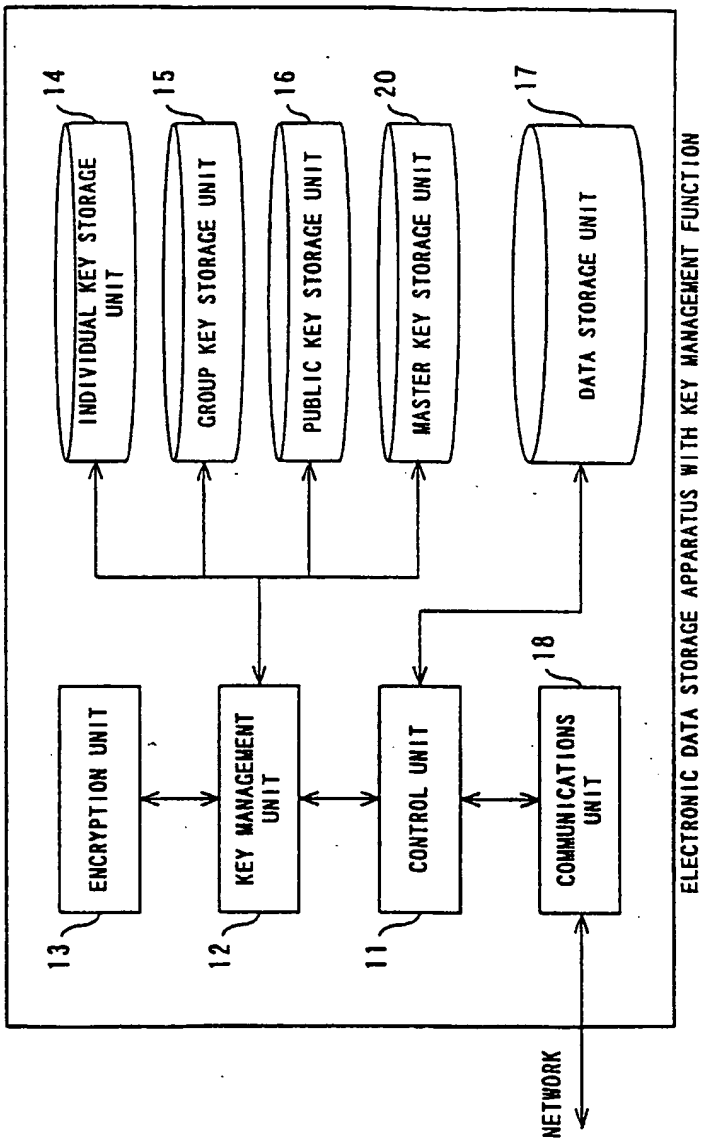
ELECTRONIC DATA STORAGE APPARATUS WITH KEY MANAGEMENT FUNCTION
INDIVIDUAL KEY STORAGE UNIT
GROUP KEY STORAGE UNIT
PUBLIC KEY STORAGE UNIT
MASTER KEY STORAGE UNIT
DATA STORAGE UNIT
ENCRYPTION UNIT
KEY MANAGEMENT UNIT
CONTROL UNIT
COMMUNICATIONS UNIT
NETWORK
14
15
16
20
17
18
13
12
11

FIG. 11

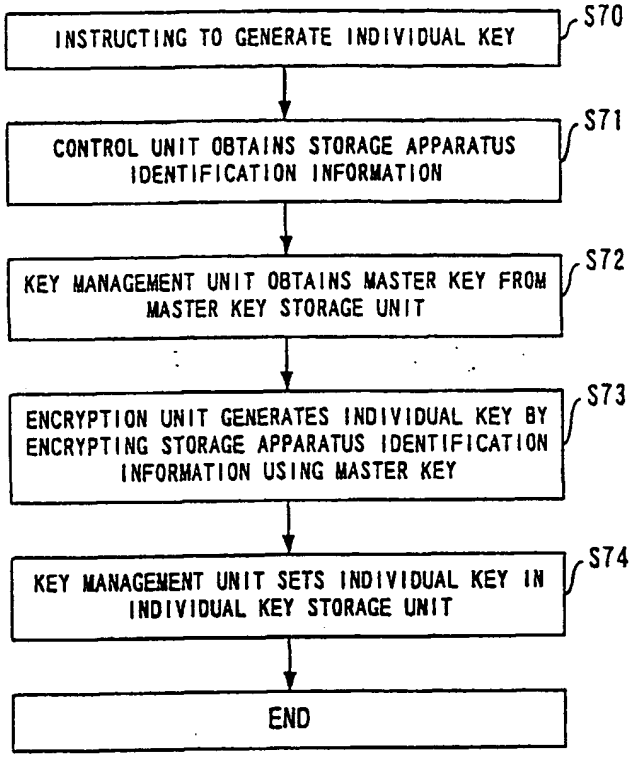
INSTRUCTING TO GENERATE INDIVIDUAL KEY
S70
CONTROL UNIT OBTAINS STORAGE APPARATUS IDENTIFICATION INFORMATION
S71
KEY MANAGEMENT UNIT OBTAINS MASTER KEY FROM MASTER KEY STORAGE UNIT
S72
ENCRYPTION UNIT GENERATES INDIVIDUAL KEY BY ENCRYPTING STORAGE APPARATUS IDENTIFICATION INFORMATION USING MASTER KEY
S73
KEY MANAGEMENT UNIT SETS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
S74
END

FIG. 12

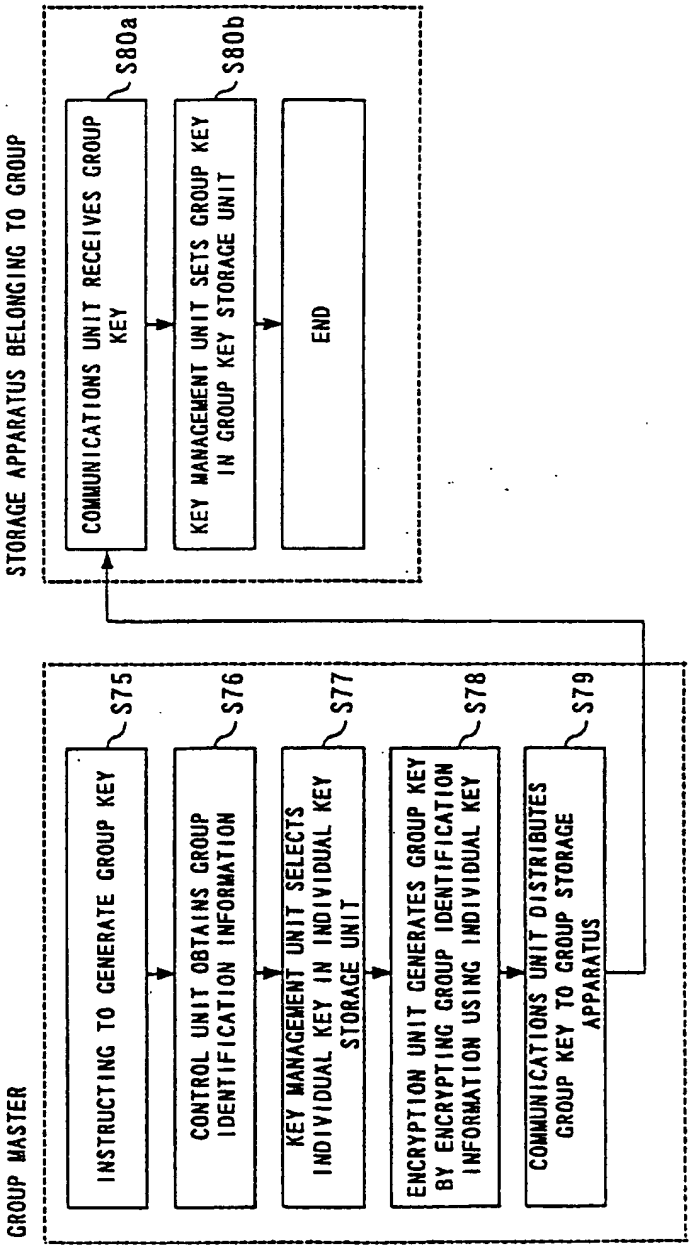
GROUP MASTER
INSTRUCTING TO GENERATE GROUP KEY
S75
CONTROL UNIT OBTAINS GROUP IDENTIFICATION INFORMATION
S76
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
S77
ENCRYPTION UNIT GENERATES GROUP KEY BY ENCRYPTING GROUP IDENTIFICATION INFORMATION USING INDIVIDUAL KEY
S78
COMMUNICATIONS UNIT DISTRIBUTES GROUP KEY TO GROUP STORAGE APPARATUS
S79
STORAGE APPARATUS BELONGING TO GROUP
COMMUNICATIONS UNIT RECEIVES GROUP KEY
S80a
KEY MANAGEMENT UNIT SETS GROUP KEY IN GROUP KEY STORAGE UNIT
S80b
END

FIG. 13

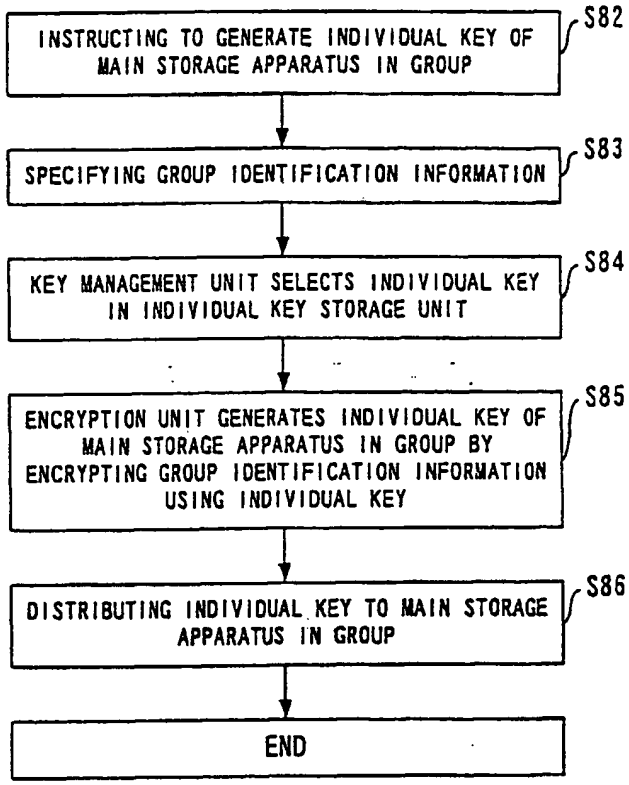
INSTRUCTING TO GENERATE INDIVIDUAL KEY OF MAIN STORAGE APPARATUS IN GROUP
S82
SPECIFYING GROUP IDENTIFICATION INFORMATION
S83
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
S84
ENCRYPTION UNIT GENERATES INDIVIDUAL KEY OF MAIN STORAGE APPARATUS IN GROUP BY ENCRYPTING GROUP IDENTIFICATION INFORMATION USING INDIVIDUAL KEY
S85
DISTRIBUTING INDIVIDUAL KEY TO MAIN STORAGE APPARATUS IN GROUP
S86
END

FIG. 14

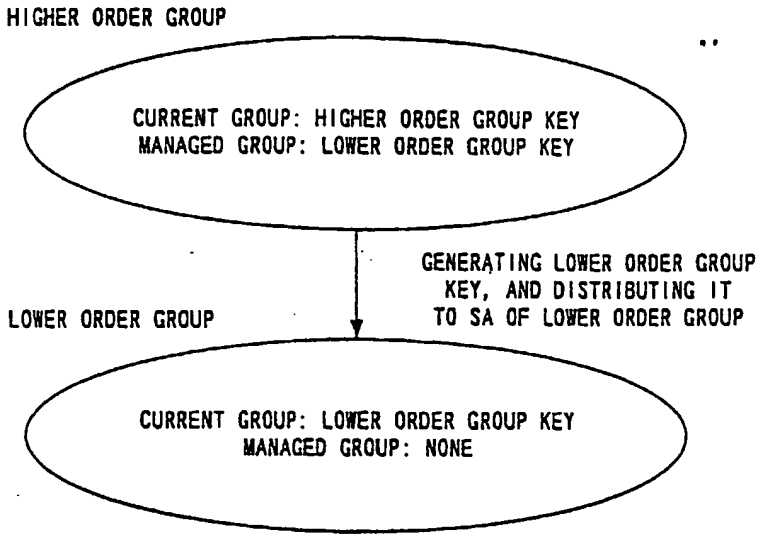
HIGHER ORDER GROUP
CURRENT GROUP: HIGHER ORDER GROUP KEY
MANAGED GROUP: LOWER ORDER GROUP KEY
GENERATING LOWER ORDER GROUP KEY, AND DISTRIBUTING IT TO SA OF LOWER ORDER GROUP
LOWER ORDER GROUP
CURRENT GROUP: LOWER ORDER GROUP KEY
MANAGED GROUP: NONE

FIG. 15

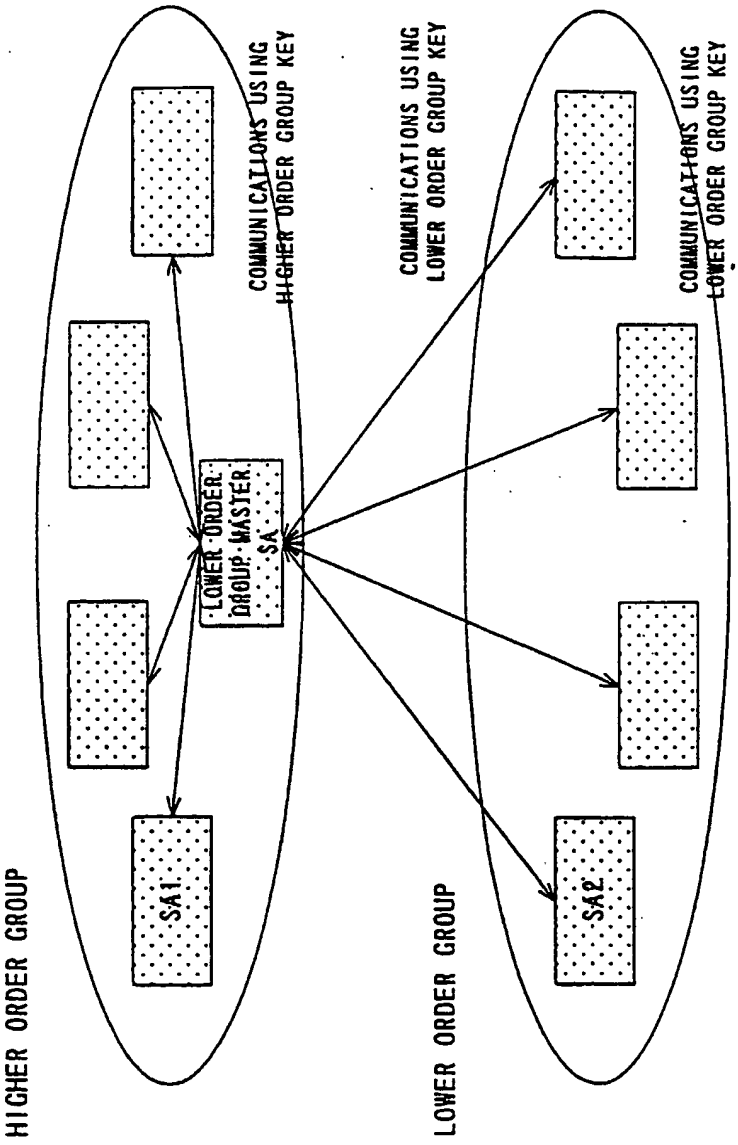
HIGHER ORDER GROUP
SA1
LOWER ORDER GROUP MASTER SA
COMMUNICATIONS USING HIGHER ORDER GROUP KEY
COMMUNICATIONS USING LOWER ORDER GROUP KEY
LOWER ORDER GROUP
SA2
COMMUNICATIONS USING LOWER ORDER GROUP KEY

FIG. 16

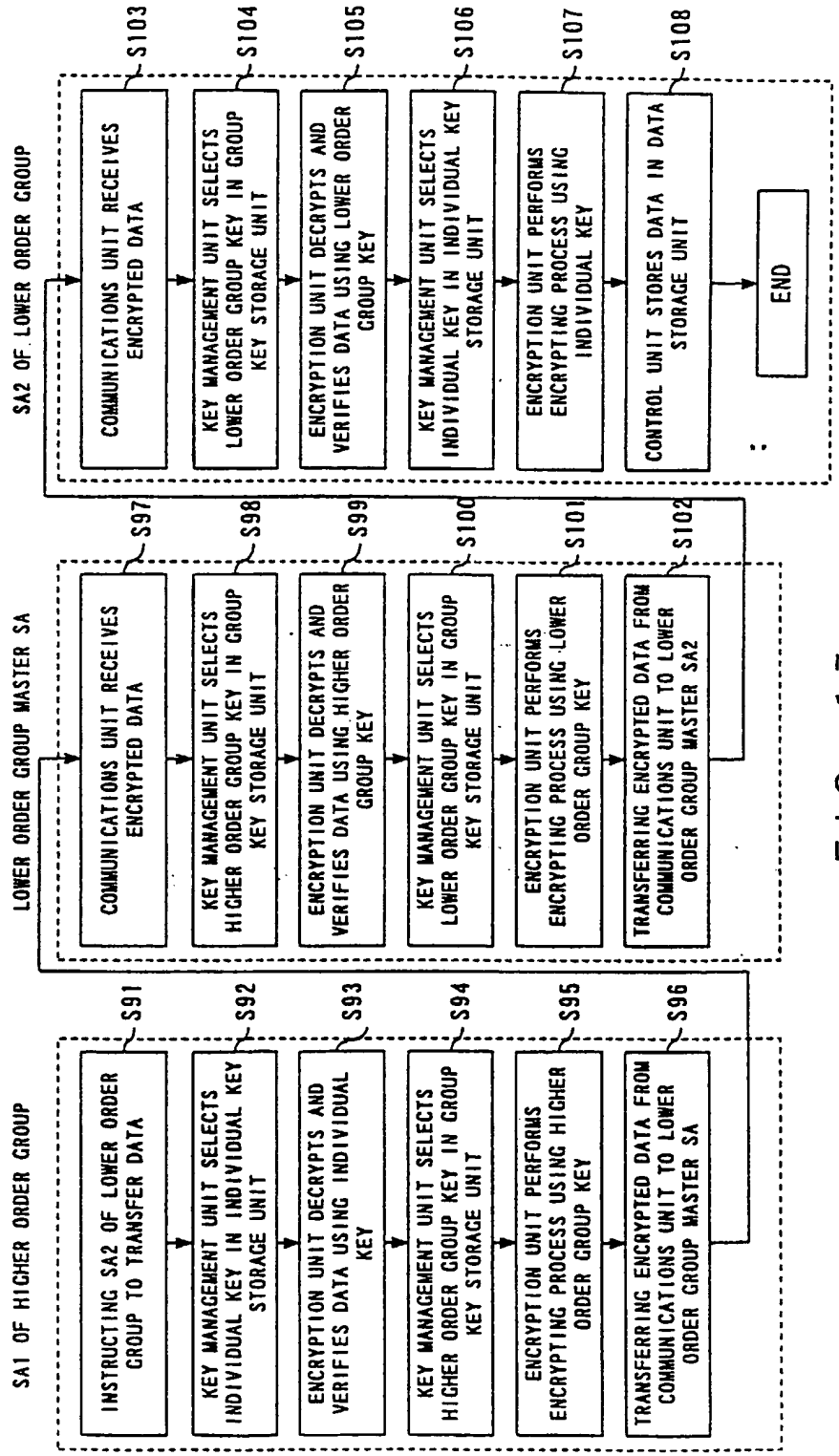
SA1 OF HIGHER ORDER GROUP
INSTRUCTING SA2 OF LOWER ORDER GROUP TO TRANSFER DATA
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING INDIVIDUAL KEY
KEY MANAGEMENT UNIT SELECTS HIGHER ORDER GROUP KEY IN GROUP KEY STORAGE UNIT
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING HIGHER ORDER GROUP KEY
TRANSFERRING ENCRYPTED DATA FROM COMMUNICATIONS UNIT TO LOWER ORDER GROUP MASTER SA
S91
S92
S93
S94
S95
S96
LOWER ORDER GROUP MASTER SA
COMMUNICATIONS UNIT RECEIVES ENCRYPTED DATA
KEY MANAGEMENT UNIT SELECTS HIGHER ORDER GROUP KEY IN GROUP KEY STORAGE UNIT
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING HIGHER ORDER GROUP KEY
KEY MANAGEMENT UNIT SELECTS LOWER ORDER GROUP KEY IN GROUP KEY STORAGE UNIT
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING LOWER ORDER GROUP KEY
TRANSFERRING ENCRYPTED DATA FROM COMMUNICATIONS UNIT TO LOWER ORDER GROUP MASTER SA2
S97
S98
S99
S100
S101
S102
SA2 OF LOWER ORDER GROUP
COMMUNICATIONS UNIT RECEIVES ENCRYPTED DATA
KEY MANAGEMENT UNIT SELECTS LOWER ORDER GROUP KEY IN GROUP KEY STORAGE UNIT
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING LOWER ORDER GROUP KEY
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING INDIVIDUAL KEY
CONTROL UNIT STORES DATA IN DATA STORAGE UNIT
END
S103
S104
S105
S106
S107
S108

FIG. 17

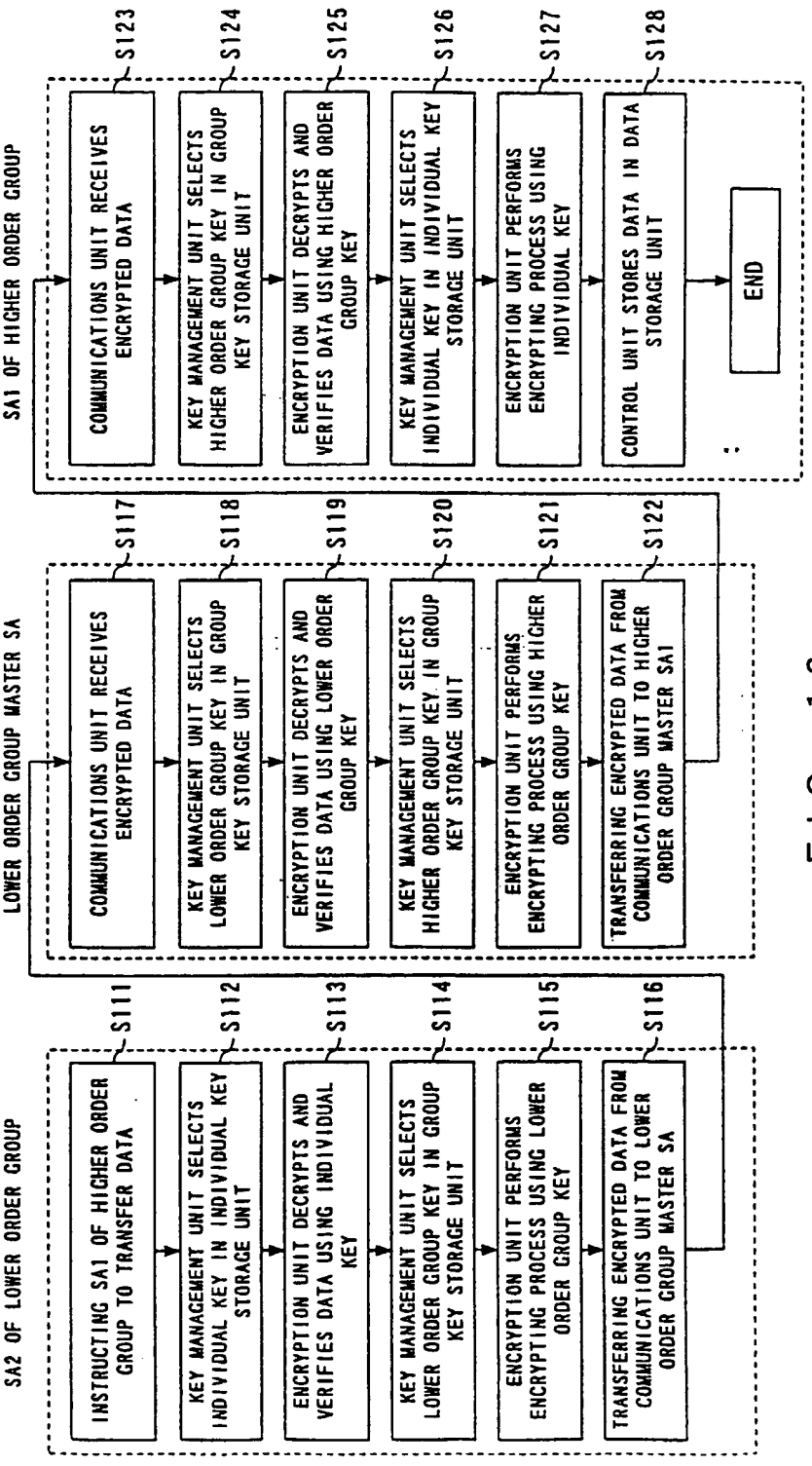
SA2 OF LOWER ORDER GROUP
INSTRUCTING SA1 OF HIGHER ORDER GROUP TO TRANSFER DATA
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING INDIVIDUAL KEY
KEY MANAGEMENT UNIT SELECTS LOWER ORDER GROUP KEY IN GROUP KEY STORAGE UNIT
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING LOWER ORDER GROUP KEY
TRANSFERRING ENCRYPTED DATA FROM COMMUNICATIONS UNIT TO LOWER ORDER GROUP MASTER SA
S111
S112
S113
S114
S115
S116
LOWER ORDER GROUP MASTER SA
COMMUNICATIONS UNIT RECEIVES ENCRYPTED DATA
KEY MANAGEMENT UNIT SELECTS LOWER ORDER GROUP KEY IN GROUP KEY STORAGE UNIT
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING LOWER ORDER GROUP KEY
KEY MANAGEMENT UNIT SELECTS HIGHER ORDER GROUP KEY IN GROUP KEY STORAGE UNIT
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING HIGHER ORDER GROUP KEY
TRANSFERRING ENCRYPTED DATA FROM COMMUNICATIONS UNIT TO HIGHER ORDER GROUP MASTER SA1
S117
S118
S119
S120
S121
S122
SA1 OF HIGHER ORDER GROUP
COMMUNICATIONS UNIT RECEIVES ENCRYPTED DATA
KEY MANAGEMENT UNIT SELECTS HIGHER ORDER GROUP KEY IN GROUP KEY STORAGE UNIT
ENCRYPTION UNIT DECRYPTS AND VERIFIES DATA USING HIGHER ORDER GROUP KEY
KEY MANAGEMENT UNIT SELECTS INDIVIDUAL KEY IN INDIVIDUAL KEY STORAGE UNIT
ENCRYPTION UNIT PERFORMS ENCRYPTING PROCESS USING INDIVIDUAL KEY
CONTROL UNIT STORES DATA IN DATA STORAGE UNIT
END
S123
S124
S125
S126
S127
S128

FIG. 18

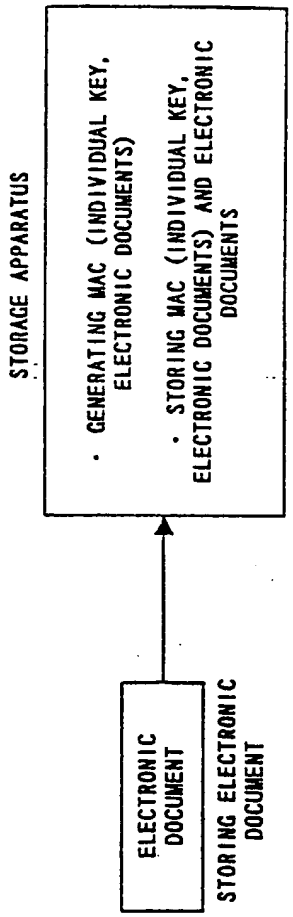
STORAGE APPARATUS
• GENERATING MAC (INDIVIDUAL KEY, ELECTRONIC DOCUMENTS)
• STORING MAC (INDIVIDUAL KEY, ELECTRONIC DOCUMENTS) AND ELECTRONIC DOCUMENTS
ELECTRONIC DOCUMENT
STORING ELECTRONIC DOCUMENT

FIG. 19

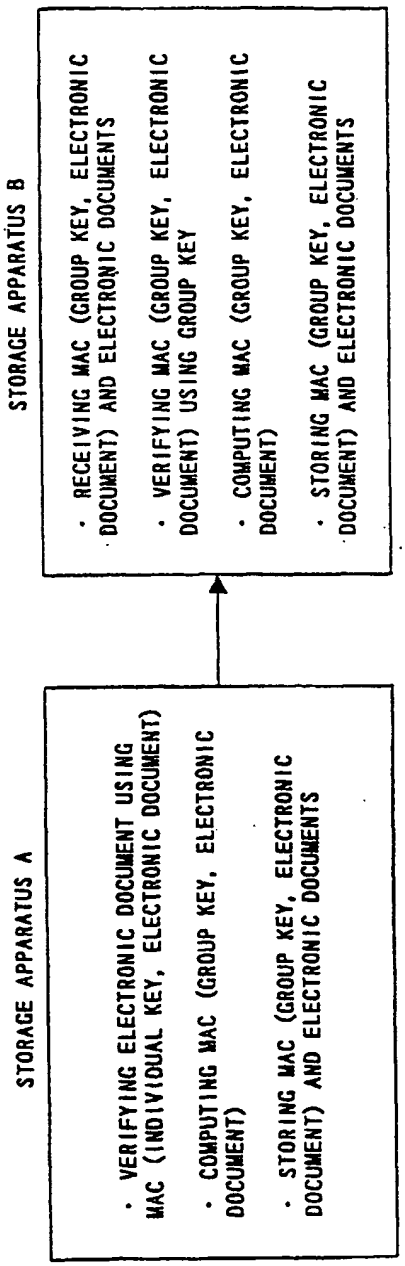
STORAGE APPARATUS A
• VERIFYING ELECTRONIC DOCUMENT USING MAC (INDIVIDUAL KEY, ELECTRONIC DOCUMENT)
• COMPUTING MAC (GROUP KEY, ELECTRONIC DOCUMENT)
• STORING MAC (GROUP KEY, ELECTRONIC DOCUMENT) AND ELECTRONIC DOCUMENTS
STORAGE APPARATUS B
• RECEIVING MAC (GROUP KEY, ELECTRONIC DOCUMENT) AND ELECTRONIC DOCUMENTS
• VERIFYING MAC (GROUP KEY, ELECTRONIC DOCUMENT) USING GROUP KEY
• COMPUTING MAC (GROUP KEY, ELECTRONIC DOCUMENT)
• STORING MAC (GROUP KEY, ELECTRONIC DOCUMENT) AND ELECTRONIC DOCUMENTS

FIG. 20

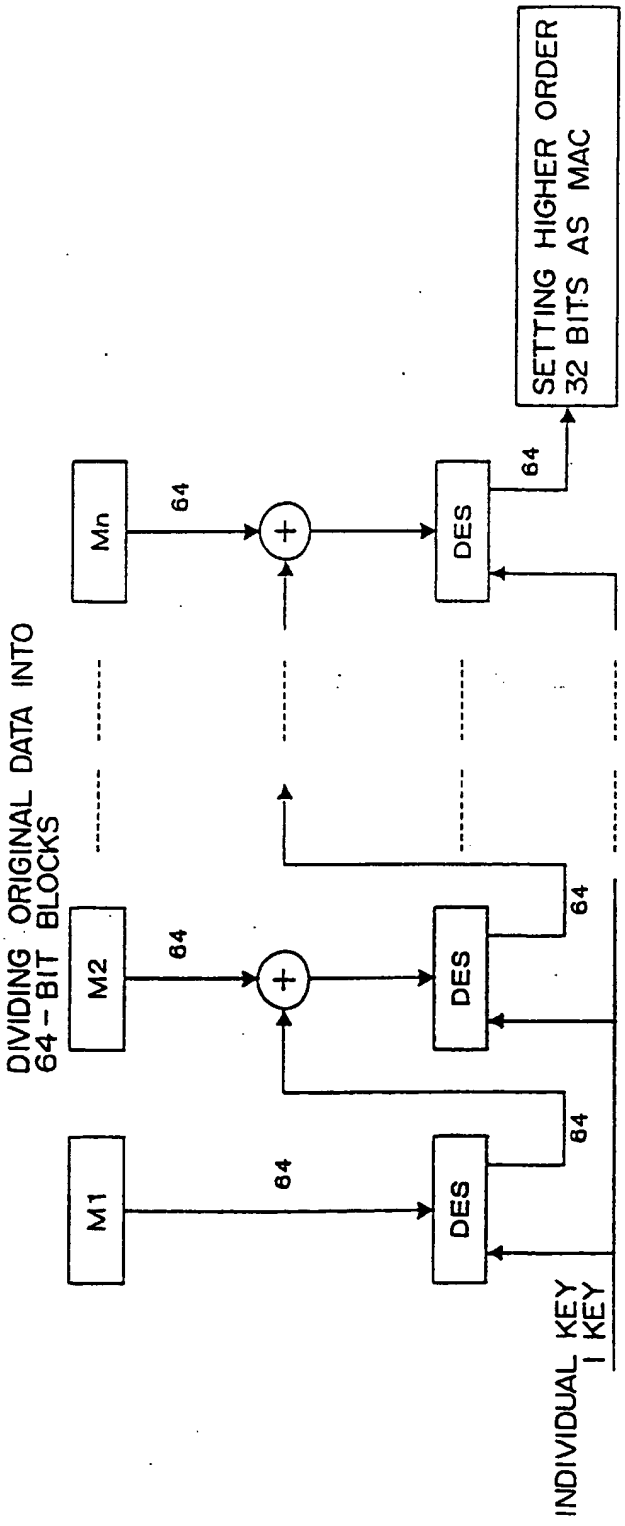
DIVIDING ORIGINAL DATA INTO 64-BIT BLOCKS
M1
M2
Mn
64
DES
SETTING HIGHER ORDER 32 BITS AS MAC
INDIVIDUAL KEY
I KEY
: EXCLUSIVE LOGICAL SUM
: DES (DATA ENCRYPTION STANDARD) PROCESS

FIG. 21

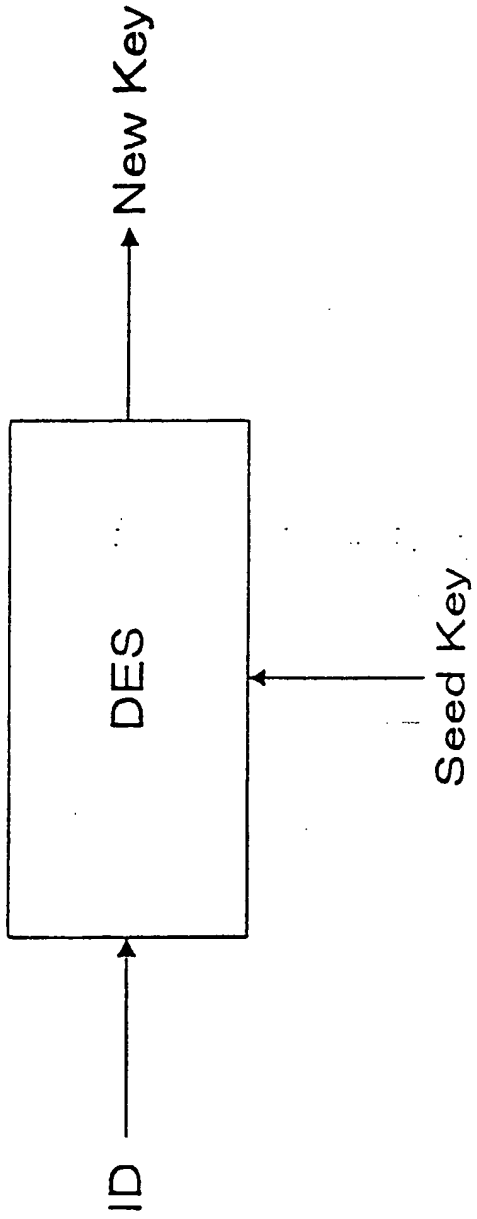

FIG. 22

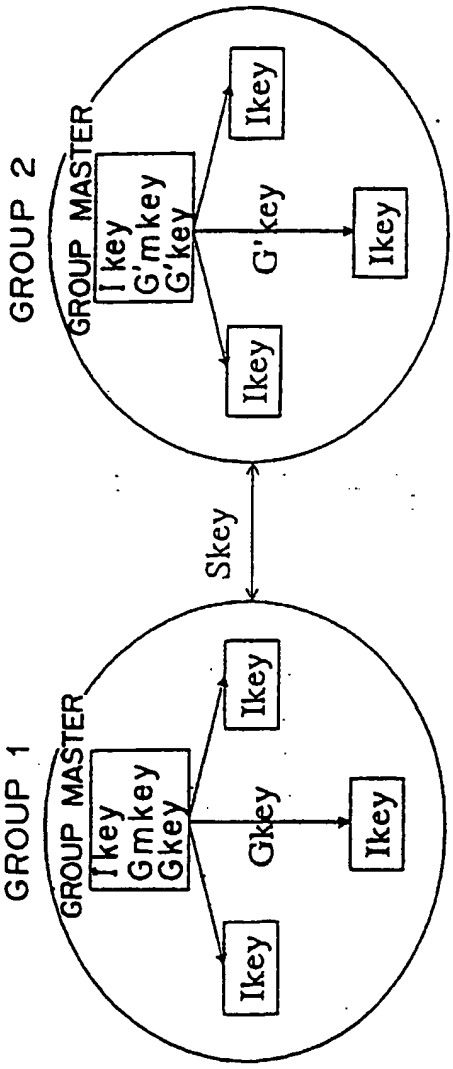
GROUP 2
GROUP MASTER
I key
G'm key
G'key
G'key
Ikey
Ikey
Ikey
Ikey
Skey
GROUP 1
GROUP MASTER
Ikey
Gmkey
Gkey
Gkey
Ikey
Ikey
Ikey
Ikey

FIG. 23

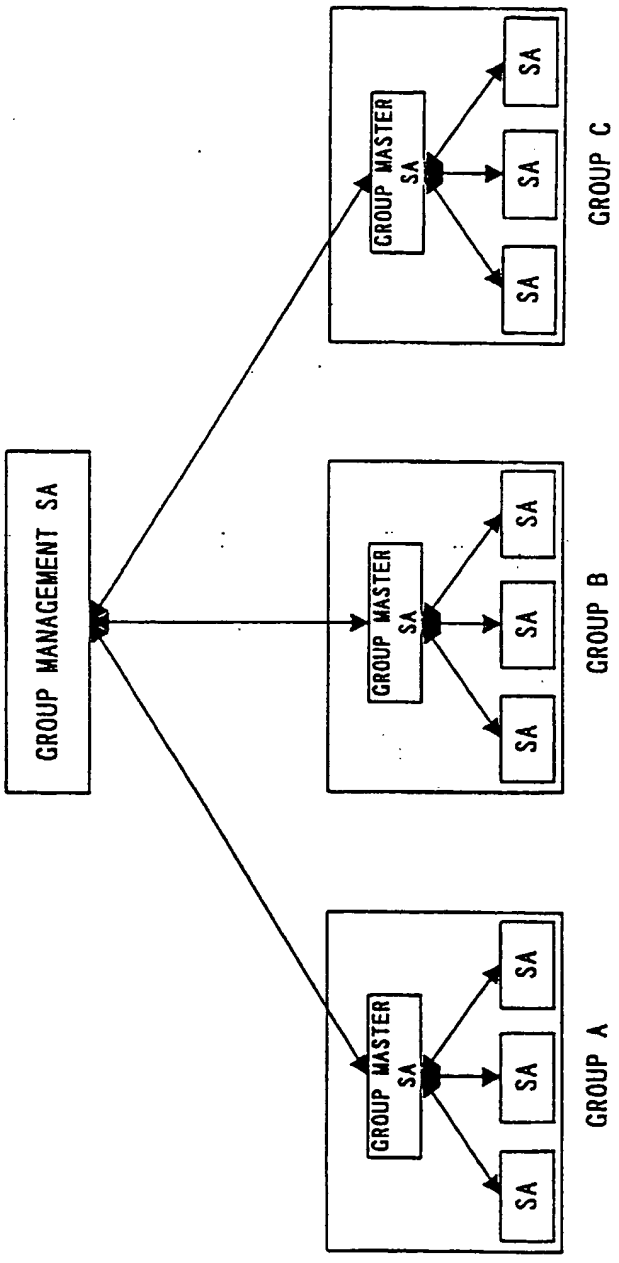
GROUP MANAGEMENT SA
GROUP MASTER SA
SA
SA
SA
GROUP A
GROUP MASTER SA
SA
SA
SA
GROUP B
GROUP MASTER SA
SA
SA
SA
GROUP C

FIG. 24